

ILLINOIS HEALTH INFORMATION EXCHANGE AUTHORITY



PRIVACY & SECURITY POLICIES & PROCEDURES

ILHIE Authority Privacy and Security Policies and Procedures

| POLICY | DESCRIPTION | PAGE |
|------------|---|------|
| | Definitions | 1 |
| Policy # 1 | Compliance with Law and Policy..... | 6 |
| Policy #2 | ILHIE Privacy and Security Governance..... | 8 |
| Policy #3 | ILHIE User Authentication..... | 10 |
| Policy #4 | ILHIE User Authorization..... | 12 |
| Policy #5 | Request, Use, and Disclosure of Protected Health Information..... | 15 |
| Policy #6 | Patient Choice and Meaningful Disclosure..... | 19 |
| Policy #7 | Information Subject to Special Protection..... | 25 |
| Policy #8 | Emergency Access..... | 27 |
| Policy #9 | Individual Access to Data..... | 29 |
| Policy #10 | Individual Amendment of Data..... | 31 |
| Policy #11 | Individual Accounting of Disclosures..... | 34 |
| Policy #12 | Minimum Necessary..... | 37 |
| Policy #13 | ILHIE Workforce, Contractors, Subcontractors, and Agents..... | 39 |
| Policy #14 | Complaint Handling and Resolution..... | 41 |
| Policy #15 | Sanctions..... | 45 |
| Policy #16 | Enforcement | 49 |
| Policy #17 | Physical Safeguards..... | 52 |
| Policy #18 | Encryption..... | 55 |
| Policy #19 | Risk Analysis and Management..... | 57 |
| Policy #20 | Information Systems Activity Review..... | 59 |
| Policy #21 | Breach Notification and Mitigation..... | 62 |
| Policy #22 | Contingency Plan..... | 72 |

For the purposes of these Policies and Procedures, the following definitions apply. Terms used, but not otherwise defined shall have the same meaning as set forth in HIPAA.

“Active Individual” or “Active Patient” means a patient of a Participant who has sought Treatment from that Participant, or one of that Participant’s Authorized User(s), who is a Health Care Provider, within the prior twenty-four (24) months.

“Applicable Law” means HIPAA, the HITECH Act, and other applicable federal and Illinois law and regulations, as amended or modified from time to time, including but not limited to the Illinois Health Information Exchange and Technology Act (20 ILCS 3860/).

“Audit Log” means the chronological sequence of audit records, each of which contains data about a specific event.

“Authorized User” means members of a Participant’s Workforce, a Participant’s agents, contractors, Subcontractors or other persons or entities authorized by such Participant, under the procedures set forth in the Data Sharing Agreement, to request, Use or Disclose Protected Health Information from Another Participant’s System. Alternatively, as appropriate in context, Authorized User means those members of the ILHIE Authority’s Workforce, the ILHIE Authority’s agents, contractors, Subcontractors or other persons or entities authorized by the ILHIE Authority to request, Use or Disclose Protected Health Information that is transmitted through the ILHIE, or those members of Another Participant’s Workforce, such Other Participant’s agents, contractors, Subcontractors or other persons or entities authorized by the Other Participant to request, Use or Disclose Protected Health Information that is transmitted through the ILHIE.

“Affected Participant” means any Participant (other than a Breaching Participant) with respect to which a Breach has occurred or for which there is a reasonable possibility that a Breach has occurred with respect to its Systems or Protected Health Information, but which does not involve an act or omission of the Affected Participant or any of its Authorized Users, Workforce, Business Associates, or Subcontractors that caused the Breach.

“Breach” means any acquisition, access, use, or disclosure of Protected Health Information which utilizes ILHIE technology or infrastructure or which allows unauthorized access to ILHIE technology, ILHIE infrastructure or Protected Health Information through the ILHIE, and which compromises the security or privacy of such information except as set forth in 45 C.F.R §164.402. A acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted by the Data Sharing Agreement, HIPAA, PIPA or other Applicable Law is presumed to be a Breach, unless the Breaching Participant or the ILHIE Authority demonstrates that there is low probability that Protected Health Information has been compromised based on a risk assessment using the factors set forth in 45 C.F.R §164.402 and the Breaching Participant or the ILHIE Authority demonstrates that the acquisition, access, use, or disclosure does not constitute a Breach under HIPAA, PIPA or other Applicable Law.

“Breaching Participant” means a Participant whose act or omission, or the act or omission of that Participant’s Authorized User, Workforce member, Business Associate, or Subcontractor, caused a Breach.

“Data Sharing Agreement” or **“DSA”** means the data sharing agreement entered into by and between the ILHIE Authority and a Participant for the use of ILHIE Connect.

“Deactivation Notice” means the notification given by the ILHIE Authority to a Participant informing the Participant that an Authorized User of the Participant will no longer be able to access Protected Health Information through ILHIE.

“Department of Health and Human Services” or **“HHS”** means the United States Department of Health and Human Services.

“EHR” means electronic health record.

“Health Information Exchange” or **“HIE”** means a Health Information Exchange as defined in the Illinois Mental Health and Developmental Disabilities Confidentiality Act (740 ILCS 110/) and any regulations promulgated or standards developed thereunder, as amended from time to time, and any other health information exchange including but not limited to federal HIEs and HIEs in states other than Illinois, that have executed a data sharing agreement with the ILHIE Authority.

“HIPAA” means, without limitation, the federal Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191) and its implementing regulations on privacy and security found at 45 C.F.R. Parts 160 and 164, as the same may be amended from time to time, including modifications to the HIPAA Security and Privacy Rules arising from the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5).

“HITECH” means the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005, and any and all regulations promulgated thereunder, as amended from time to time.

“ILHIE” means the Illinois Health Information Exchange as established by the Illinois Health Information Exchange and Technology Act, and any and all regulations promulgated thereunder, as amended from time to time.

“ILHIE Authority” means the Illinois Health Information Exchange Authority as established by the Illinois Health Information Exchange and Technology Act. Unless otherwise specified, “ILHIE Authority” shall include its Workforce, contractors, Subcontractors, and Business Associates.

“ILHIE Connect” means the ILHIE Authority’s ILHIE Connect service, a State-wide bi-directional health information exchange.

“ILHIE Breach” shall mean a Breach of the ILHIE during the transmission of Protected Health Information through the ILHIE or a Breach due to the act or omission of the ILHIE Authority. An ILHIE Breach does not include a Breach of the ILHIE that did not occur during

transmission through the ILHIE or a Breach that is not due to the act or omission by the ILHIE Authority.

“ILHIE Notice” means written notice developed and approved by the ILHIE Authority for use by Participants to provide Active Patients with meaningful disclosure about ILHIE Connect and that explains the function of ILHIE Connect, the purposes for disclosure of a patient’s Protected Health Information to Another Participant, the potential benefits and risks to an Individual of participation in ILHIE Connect and any other information as required by law. The ILHIE Notice will further explain an Individual’s right to opt out of ILHIE Connect and directs the Individual to the ILHIE Authority’s website containing (i) an explanation of the purposes of the health information exchange and (ii) audio, visual, and written instructions on how to opt out of ILHIE Connect.

“ILHIE PCO” means the ILHIE Privacy and Compliance Officer or other individual designated by the ILHIE Authority.

“ILHIE Signage” means signage developed and approved by the ILHIE Authority that briefly describes ILHIE Connect, Individual opt-out rights, and that identifies the ILHIE Authority website.

“Informational Notification” means the notification that a Breaching Participant gives to ILHIE Authority and Affected Participants. Informational Notification should be contrasted to “Legal Notification” which is that notification required by HIPAA, HITECH and other Applicable Law.

“Legal Notification” means notification required by law to be made in the event of a Breach.

“Master Patient Index” means the Master Patient Index that is maintained by the ILHIE Authority which holds (i) demographic information about each Individual enrolled by a Participant, (ii) a list of each such Individual’s health care providers that are Participants, and (iii) each such Individual’s consent preference with regard to each Participant.

“Meaningful Use” or “Meaningful Use Regulations” means the regulations put forth by the Centers for Medicare & Medicaid Services in the final rule on meaningful use, found at 42 C.F.R. Parts 412, 413, 422, and 495, and the regulations put forth by the Office of the National Coordinator for Health Information Technology, found at 45 C.F.R. Part 170.

“National Institute of Standards and Technology” or “NIST” means the non-regulatory federal agency within the U.S. Department of Commerce.

“Opt-Out Form” means the “Illinois Health Information Exchange Authority’s ILHIE Connect Opt-Out Form” developed and approved by the ILHIE Authority for use to document a Individual’s ILHIE Connect opt-out decision, and which may be updated from time to time.

“Opt-In Form” means the “Illinois Health Information Exchange Authority’s ILHIE Connect Opt-In Form” developed and approved by the ILHIE Authority for use to document a Individual’s ILHIE Connect opt-in decision for patients who previously did not participate in ILHIE Connect, and which may be updated from time to time.

“Other Participant” or “Another Participant” means any other individual or entity including without limitation another HIE that has signed a Data Sharing Agreement to participate in the ILHIE.

“Participant(s)” means an individual who or entity, including without limitation an HIE, that has executed a Data Sharing Agreement with the ILHIE Authority. In the future, Participants may include public and private health insurance plans.

“PIPA” means the Illinois Personal Information Protection Act (815 ILCS 5301/), and any and all regulations promulgated thereunder, as amended from time to time.

“Permitted Purpose(s)” means the following purposes for which Participant(s) and the ILHIE Authority are authorized to access, acquire, request, use, and/or disclose Protected Health Information through the ILHIE: (i) Treatment of the Individual who is the subject of the Protected Health Information; (ii) Payment activities of the Health Care Provider for the Individual who is the subject of the Protected Health Information; (iii) Health Care Operations; (iv) public health activities and reporting as permitted by HIPAA and other Applicable Law; (v) any purpose to demonstrate meaningful use of certified electronic health record technology in accordance with the Meaningful Use Regulations; and (vi) uses and disclosures pursuant to an Authorization provided by the Individual who is the subject of the Protected Health Information or such Individual’s personal representative as described in 45 C.F.R §164.502(g) of the HIPAA regulations. Protected Health Information shall be accessed, acquired, requested, used and disclosed in compliance with the Data Sharing Agreement, these Policies and Procedures, and Applicable Law. At this time, there is no secondary data use allowed. Any purpose that is not a Permitted Purpose is a secondary data use.

“Policies and Procedures” means these Policies and Procedures which are the ILHIE Authority standards, policies and procedures adopted by the ILHIE Authority, as updated, changed or supplemented from time to time.

“Specially Protected Health Information” means alcohol and substance abuse treatment information that is protected under federal or Illinois law, HIV test results and the identity of the tested patient, genetic testing and information, child abuse and neglect reports and records, sexual assault evidence and information, veteran’s homes resident records, and all other health information that requires specific written patient consent for disclosure under federal or Illinois law, as amended from time to time.

“System” or “Information System” means an interconnected set of information resources under the same direct management control that shares common functionality. A System normally includes hardware, software, information, data, applications, communications, and people. For purposes of these Policies and Procedures, a System is the System by which Participant holds or exchanges Protected Health Information under this Agreement. For purposes of these Policies and Procedures, it shall not matter whether Participant controls or utilizes the System through ownership, lease, license, or otherwise. Where appropriate in context, “System” or “Information System” shall also mean the ILHIE Authority system.

“System Administrator” means the authorized individual(s) who has been assigned primary responsibility for maintaining and managing a System.



| |
|---|
| Policies and Procedures |
| POLICY: Compliance with Law and Policy |
| Policy #1 |
| Effective Date: April 2, 2014 |

Purpose: This policy defines and clarifies ILHIE Authority and Participant responsibilities to use ILHIE technology and the infrastructure supporting the ILHIE in an appropriate and lawful manner.

Policy: The ILHIE Authority and all Participants shall comply with Applicable Law related to the activities of the ILHIE, and with these Policies and Procedures.

- 1.0 Laws.** Participants must, at all times, comply with Applicable Law, including, but not limited to, those protecting the confidentiality and security of Protected Health Information and establishing Individual privacy rights.
- 2.0 ILHIE Authority Policy.** Prior to participation, Participants shall execute and comply with the Data Sharing Agreement or other applicable agreements with the ILHIE Authority, which establishes the mutual responsibilities of the ILHIE Authority and the Participant.
 - 2.1** Participants who have executed a Data Sharing Agreement and agree to the terms and conditions stated therein must comply with all Policies and Procedures, the Data Sharing Agreement, including the ILHIE On-Boarding Manual, and Applicable Law.
 - 2.2** In the event of a conflict between these Policies and Procedures and the Participant's own policies and procedures, the Participant shall comply with the policy and procedure that better protects an Individual's Protected Health Information, as determined by the Participant in cooperation with the ILHIE Authority.
 - 2.3** Except as set forth in 2.2 above, a Participant's material noncompliance with these Policies and Procedures may result in the suspension or revocation of all rights of the Participant, including the Participant's Authorized Users, to access the ILHIE or in the termination of the Data Sharing Agreement in accordance with the terms of the Data Sharing Agreement.
- 3.0 Participant Policy.** Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with these Policies and Procedures, the Data Sharing Agreement, including the ILHIE On-Boarding Manual, and Applicable Law.
- 4.0 Participation in Other Health Information Exchanges.** Participant shall cooperate with the ILHIE Authority regarding compliance related to any other national or interstate health information exchange, including but not limited to the eHealth Exchange, in which the Authority participates.

5.0 HIPAA. The implementation specifications set forth in the HIPAA Security Rule are classified as "Required" or "Addressable".

5.1 The ILHIE Authority shall meet the Required and the Addressable implementation specifications. In the event that it is not reasonable and appropriate for the ILHIE Authority to meet an Addressable implementation specification, the ILHIE Authority shall document why it would not be reasonable and appropriate to implement the specification and shall implement an equivalent alternative measure.

5.2 Participants shall meet the Required HIPAA implementation specifications. Participants shall meet the Addressable implementation specifications to the extent required under HIPAA. In the event that it is not reasonable and appropriate for a Participant to meet an Addressable implementation specification under HIPAA, the Participant shall document why it would not be reasonable and appropriate to implement the specification and implement an equivalent alternative measure, if appropriate.

6.0 Application to Business Associates and Contractors. Participants shall require its Business Associates and Subcontractors of its Business Associates to comply with these Policies and Procedures.

7.0 Compliance. Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

7.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies and References

45 C.F.R §164 Parts 160, 162, and 164

Data Sharing Agreement

Enforcement

Sanctions

Definitions

Applicable Law

Authorized User

Business Associate

ILHIE Authority

Participant

Policies and Procedures

Protected Health Information



| |
|--|
| Policies and Procedures |
| POLICY: ILHIE Authority Privacy and Security Governance |
| Policy #2 |
| Effective Date: April 2, 2014 |

Purpose: This policy defines the ILHIE Authority's privacy and security governance processes.

The Illinois Health Information Exchange and Technology Act (20 ILCS 3860/20) delegates the following powers and responsibilities, among others, to the ILHIE Authority regarding the protection of the privacy and security of Protected Health Information:

- (i) "The Authority shall establish and adopt standards and requirements for the use of health information and the requirements for participation in the ILHIE;
- (ii) The Authority shall establish minimum standards for accessing the ILHIE to ensure that the appropriate security and privacy protections apply to health information;
- (iii) The Authority shall have the power to suspend, limit, or terminate the right to participate in the ILHIE for non-compliance or failure to act, with respect to applicable standards and laws, in the best interests of patients, users of the ILHIE, or the public; and
- (iv) The Authority may seek all remedies allowed by law to address any violation of the terms of participation in the ILHIE."

Policy:

1.0 ILHIE Authority Board. The ILHIE Authority Board shall review the ILHIE Authority Data Security and Privacy Committee recommendations regarding these Policies and Procedures.

1.1 Amendments to the Policies and Procedures shall be effective when adopted by the ILHIE Authority Board, ordinarily following input from the ILHIE Authority Data Security and Privacy Committee. Participant shall comply with amendment(s) no less than 30 days of the effective date unless otherwise specified.

1.2 The ILHIE Authority shall notify Participants of all changes to these Policies and Procedures electronically by notice posted on the ILHIE website and other means deemed appropriate by the ILHIE Authority Board.

2.0 ILHIE Data Security and Privacy Committee. The ILHIE Authority Data Security and Privacy Committee of the ILHIE Authority Board was created by ILHIE Authority Board Resolution No. 2011-12. The Committee is charged with reviewing and recommending policies to the ILHIE Authority Board with regard to the use and protection of health information created, received, maintained or transmitted by the ILHIE.

2.1 The ILHIE Authority Data Security and Privacy Committee shall review and recommend, at a minimum annually, the creation, modification or amendment

of the Policies and Procedures in response to changes in Applicable Law, changes in technology and standards, changes in available compliance mechanisms, other factors affecting the governance and operation of the ILHIE, in response to identified Breaches, and other appropriate reasons. (See also ILHIE Authority Board Resolution No. 2014-04).

3.0 ILHIE Authority Privacy and Compliance Officer. The ILHIE Authority shall appoint one or more individuals who will be responsible for the development and implementation of privacy and security policies and procedures.

3.0 Compliance. Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

3.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

4.0 Conflict. If there is conflict between these Policies and Procedures and the terms of the Data Sharing Agreement, the Policies and Procedures shall control.

Associated Policies and References

Illinois Health Information Exchange and Technology Act, 20 ILCS 3860

ILHIE Authority Resolution 2011-12

Data Sharing Agreement

Enforcement

Sanctions

Definitions

Applicable Law

Breach

Participant

Protected Health Information

Purpose: This policy describes ILHIE Authority and Participant responsibilities as related to authentication of an Authorized User's identity for the purposes of verification in order to prevent unauthorized users from accessing Protected Health Information available through the ILHIE.

Policy: The ILHIE Authority and Participants shall each verify the identity of its respective Authorized Users consistent with National Institute of Standards and Technology ("NIST") Level 3 guidelines. NIST Level 3 authentication should be in accordance with the NIST Special Publication 800-63-2 Electronic Authentication Guideline, as revised from time to time.

- 1.0 Authentication.** The ILHIE Authority and Participants shall each implement user authentication policies and procedures for the purposes of verification of its respective Authorized Users as a prerequisite to permitting an Authorized User to access the ILHIE.
 - 1.1** The ILHIE Authority and Participants shall each designate Authorized Users within their respective organizations that will be authorized to access information available through the ILHIE.
 - 1.2** Each of Participant's Authorized User must be appropriately authenticated by its Participant's System or directly authenticated by the ILHIE System in order to access the ILHIE. The ILHIE Authority will grant Participant Authorized User(s) access to the ILHIE through the Participant's System in reliance upon the Authorized User's authentication through the Participant's System.
 - 1.3** The ILHIE Authority shall verify and authenticate Participant System Administrators in accordance with NIST Level 3 guidelines.
 - 1.4** The ILHIE Authority and each Participant shall verify and authenticate its respective Authorized Users using appropriate identification and authentication procedures in accordance with the NIST Level 3 guidelines.
- 2.0 Password Controls.** The ILHIE Authority and Participants shall each implement and enforce internal policies applicable to its respective Authorized Users governing the use of unique identifiers and passwords.
 - 2.1** All Authorized Users shall be assigned unique identifiers and passwords.
 - 2.2** Consistent with industry and government best practices, the ILHIE Authority and Participants shall each implement Authorized User password procedures including, but not limited to, password strength requirements; re-setting and re-use of passwords; response to failed access attempts including a lock-out mechanism; automatic log-offs; and log-in monitoring to protect against

password guessing. Authorized Users shall be required to keep their user names, passwords and other security measures for connectivity confidential.

- 3.0 Information Systems Activity Review.** The ILHIE Authority shall generate audit logs of the ILHIE System in a standardized format such as Audit Trail and Node Authentication (ATNA) to record Authorized User ILHIE System access and activity.
- 3.1** Participant shall generate audits logs in a standardized format such as ATNA to record Authorized User ILHIE System access and activity from Participant's System, and upon reasonable request make available to the ILHIE Authority such audit logs for the purpose of matching against the ILHIE audit log. Participant shall review the generated audit logs on a routine basis.
- 3.2** The ILHIE Authority and Participants shall implement authentication mechanisms in accordance with the Information Systems Activity Review Policy (Policy #20) to consistently pass along ILHIE Authority compliant authentication information.
- 4.0 ILHIE Authority Review.** The ILHIE Authority has the right to review Participant authentication policies and may audit Participants for compliance at any time.
- 5.0 Compliance.** Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
- 5.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Polices and References:

45 C.F.R §164.312(a); 45 C.F.R §164.312(d)
Breach Notification and Mitigation
Enforcement
Information Systems Activity Review
Sanctions
User Authorization

Definitions

Authorized Users
ILHIE Authority
NIST
Participant
Protected Health Information
System Administrator

Purpose: This policy describes the duty of the ILHIE Authority and Participant to define the requirements for establishing user access controls and other technical safeguards to ensure user authorization.

Policy: The ILHIE Authority shall grant Participants access to the ILHIE as set forth in these Policies and Procedures and the Data Sharing Agreement. Access rights shall be based on individual roles and job responsibilities.

1.0 Access Controls. Consistent with the Permitted Purposes, the ILHIE Authority and Participants shall implement technical policies and procedures to allow ILHIE access only to those Authorized Users or software programs that have been granted access rights.

1.1 The ILHIE Authority shall implement and communicate to Participants specific role classifications to which a Participant may assign Authorized Users and the specific System permissions associated with each such classification.

1.2 Each Participant shall appoint a System Administrator. Each Participant may also appoint one or more alternate System Administrator(s). Each System Administrator must submit to an authentication and verification process as required by the ILHIE Authority in order to be granted access to the ILHIE. After successfully completing the verification process, the System Administration may create, manage, and terminate Authorized Users under the Participant's account as set forth by the ILHIE Authority.

1.3 Each Participant's System Administrator may create, manage, and revoke access to the ILHIE for its Authorized Users under the Participant's account, including through log-in/password generation and resetting in accordance with these Policies and Procedures.

1.4 The ILHIE Authority and each Participant shall provide Authorized User access only to its respective Workforce, contractors, Subcontractors and agents who have a need to request, use, or disclose Protected Health Information through the ILHIE for a Permitted Purpose.

1.5 Participants are responsible for initially creating, managing, and revoking Authorized Users in accordance with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

2.0 Authorized Users. The ILHIE Authority and Participant shall use reasonable care in selecting its respective Authorized Users and shall require that the Authorized Users act in compliance with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

2.1. Participant shall have a valid and enforceable agreement with each of its Authorized Users that require the Authorized User to, at a minimum:

- (i) Comply with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law, as applicable;
- (ii) Reasonably cooperate with the ILHIE Authority and Participant on issues related to these Policies and Procedures;
- (iii) Request, use, or disclose Protected Health Information only for a Permitted Purpose;
- (iv) Use proprietary information or Protected Health Information received from an Other Participant in accordance with these Policies and Procedures;
- (v) As soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant or if Authorized User cannot report the Breach to Participant then report the Breach to the ILHIE Authority; and
- (vi) Refrain from disclosing to any other person any passwords or other security measures issued to the Authorized User by the Participant.

Notwithstanding the foregoing, for Authorized Users who are employed by a Participant or who have agreements with the Participant which became effective prior to the effective date of the Participant's Data Sharing Agreement, compliance with this Section may be satisfied through written policies and procedures that address (i) through (vi) so long as the Participant can document that there is a written requirement that the Authorized User must comply with the Policies and Procedures.

3.0 Access Revocation and Reinstatement. Participant shall comply and require its Authorized Users to comply with the ILHIE access suspension, revocation, and reinstatement Policies and Procedures as set forth in the Sanctions Policy (Policy #15).

4.0 Breach. Participant shall comply and require its Authorized Users to comply with the Breach Notification and Mitigation Policy (Policy #21) in the event of a Breach or suspected Breach.

5.0 Training. All members of the ILHIE Authority and each Participant's respective Workforce, and their respective contractors, Subcontractors or agents, as applicable, who will have access to the ILHIE as an Authorized User, shall undergo both initial and ongoing security awareness training, to ensure compliance these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

5.1. No Workforce member, contractor, Subcontractor or agent shall be provided with access to the ILHIE, an unique identifier or a password prior to completing training.

6.0 Compliance. Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

- 6.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies and References:

45 C.F.R §164.308(a)(5)(i)

45 C.F.R §164.306(d)

Data Sharing Agreement

Access Use and Disclosure of Protected Health Information

Breach Notification and Mitigation

Enforcement

Sanctions

User Authentication

Definitions

Applicable Law

Authorized User

Participant

Protected Health Information

System Administrator

Workforce

| |
|---|
| Policies and Procedures |
| POLICY: Request, Use, and Disclosure of Protected Health Information |
| Policy #5 |
| Effective Date: April 2, 2014 |

Purpose: This policy describes the permissible uses of information available through the ILHIE to ensure that Protected Health Information and other data available through the ILHIE are appropriately secured and are requested, used, and disclosed through the ILHIE only in manner consistent with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

Policy: Participant and its Authorized Users will request, use, and disclose Protected Health Information through the ILHIE only in the manner permitted under the Data Sharing Agreement and these Policies and Procedures, and subject to any restrictions to which the Participant has agreed upon with Individuals. ILHIE Authority Authorized Users may request, use, and disclose Protected Health Information only in the manner consistent with the Data Sharing Agreement and these Policies and Procedures.

1.0 Compliance with Law. Participant shall request, use, and disclose Protected Health Information through the ILHIE only in a manner consistent with Applicable Law and not for any unlawful or discriminatory purpose.

1.1 If Applicable Law or the Policies and Procedures require that certain documentation exist or that other conditions be met prior to requesting, using, or disclosing Protected Health Information through the ILHIE for a Permitted Purpose, the Participant or its Authorized User shall ensure that it has obtained the required documentation or met the requisite conditions.

2.0 Permitted Uses and Disclosures. Participant and its Authorized Users, may request, use, or disclose Protected Health Information through the ILHIE only for a Permitted Purpose or in reasonable anticipation of a Permitted Purpose, as defined in the Data Sharing Agreement and these Policies and Procedures and only to the extent necessary and permitted by Applicable Law. At this time, there is no secondary data use allowed.

2.1 Protected Health Information received by Participant or its Authorized User for a Permitted Purpose shall not be disclosed to any third party for a non-Permitted Purpose unless required or permitted under the Data Sharing Agreement or Applicable Law.

2.2 In the absence of a Permitted Purpose, Participant and its Authorized Users may not request information through the ILHIE.

2.3 The ILHIE Authority may request, use, and disclose Protected Health Information for the following purposes:

- (i) To manage authorized requests for, and disclosures of Protected Health Information for Permitted Purposes among Participants in the ILHIE;

- (ii) Collecting, aggregating, formatting, or transmitting health information data, as Protected Health Information or in de-identified format, for public health reporting or meaningful use reporting;
- (iii) For the proper management and administration of the ILHIE Authority as a Business Associate, in accordance with 45 C.F.R §164.504(e)(4);
- (iv) To create and maintain a Master Patient Index, including to process or otherwise implement consent management processes, provide a record locator or patient matching service, and facilitate the identification and correction of errors in health information records;
- (v) To engage in any other activities reasonably related to the operation of the ILHIE that are authorized by the ILHIE Authority and are consistent with Applicable Law; or
- (vi) For any other purposes required of or permitted to the ILHIE Authority in furtherance of the ILHIE Authority's rights and duties under Applicable Law, upon the development of appropriate policies, procedures, or standards, as applicable.

3.0 Reliance. Each request for disclosure of Protected Health Information by a Participant is a representation to every Other Participant that all prerequisites under Applicable Law and under the Policies and Procedures for such request by the Participant have been met.

3.1 If Participant is unable to separate specific Protected Health Information about a particular Individual that requires additional protections or consent from Protected Health Information that does not require additional protections or consent, Participant shall not provide any Protected Health Information about that Individual through the ILHIE.

4.0 Mandatory Disclosures. The ILHIE Authority and Participants shall comply with requests for mandatory Protected Health Information disclosures in a manner consistent with Applicable Law.

4.1 Upon receiving an authorized request from a Department of Health and Human Services official for disclosure of Protected Health Information, the Participant or the ILHIE Authority will provide the requested Protected Health Information as required by and in accordance with Applicable Law. Unless expressly prohibited, the ILHIE Authority will notify the appropriate Participant(s) of the request.

5.0 Requests for Restrictions on Uses and Disclosures. Upon receiving a written request from an Individual for restriction of request, use, and disclosure of that Individual's Protected Health Information through the ILHIE, a Participant shall inform the Individual about the opt-out process described in the Patient Choice and Meaningful Disclosure Policy (Policy #6) and shall provide a copy of the Opt-Out Form to the Individual.

6.0 Prohibitions on Uses and Disclosures of Protected Health Information. Except as permitted by HIPAA, Protected Health Information may not be used by a

Participant or the ILHIE Authority for marketing, marketing-related purposes, or sales without the authorization of the Individual.

7.0 Subsequent Use and Disclosure. A Participant who has requested Protected Health Information through the ILHIE and merged the information received into its own records shall treat the merged information as part of its own record and thereafter use and disclose the merged information only in a manner consistent with its own policies and procedures and Applicable Law.

7.1 Each Participant shall refer to and comply with its own policies and procedures regarding disclosures of Protected Health Information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making subsequent disclosures of the merged information.

8.0 Authentication. Participant shall ensure its Authorized Users meet requirements for accessing data in compliance with the User Authentication Policy (Policy #3).

9.0 Compliance. Participant shall comply with these Policies and Procedures. The ILHIE Authority shall monitor and enforce compliance with and adherence to these Policies and Procedures.

9.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies and References:

45 C.F.R §164.500 et seq.
Data Sharing Agreement
Breach Notification and Mitigation
Enforcement
Individual Access to Data
Individual Accounting of Disclosure
Information Subject to Special Protection
Information Systems Activity Review
Minimum Necessary
Opt-Out Form
Patient Choice and Meaningful Disclosure
Sanctions
User Authentication

Definitions

Applicable Law
Health Care Operations
HIPAA
ILHIE Authority
Master Patient Index
Meaningful Use
Participant

Payment
Permitted Purposes
Policies and Procedures
Protected Health Information Treatment
US/DHHS

| |
|--|
| Policies and Procedures |
| POLICY: Patient Choice and Meaningful Disclosure |
| Policy #6 |
| Effective Date: November 7, 2013 |

Background and Purpose: The ILHIE Authority is committed to protecting and respecting the privacy of Individual's Protected Health Information. As part of its mission, the ILHIE Authority is statutorily required to create rules, standards, or contractual obligations that provide each Individual whose Protected Health Information are accessible through ILHIE Connect to have the option to opt out, opt in, and revoke a prior decision to opt out or opt in. These rules, standards, or contractual obligations shall require written notice of an Individual's right to opt-out which directs the Individual to an HIE website. The Individual shall be provided meaningful disclosure regarding health information exchange (740 ILCS 14/9.6).

In accordance with the statutory requirements above, this policy describes how the participation decisions of Individuals to opt out of or to opt in to the ILHIE Authority's ILHIE Connect may be meaningfully exercised at the point of care. The policy also describes how an Individual may subsequently change these participation decisions. As used in this Policy and Procedure, "Participant" may additionally mean the Participant's Authorized User, as appropriate.

Policy:

- 1.0 Patient Choice.** The ILHIE Authority will offer all Individuals a meaningful and informed way to decide whether to opt out of participation in ILHIE Connect. This Individual participation process will be governed by an opt-out policy and administered by each Participant at the point of care. Each Participant governs only the Protected Health Information held by that Participant. All Individuals that are patients of a Participant will be automatically enrolled in ILHIE Connect, and no affirmative action will need to be taken by Individuals to establish his or her participation, unless an Individual's medical record contains categories of Specially Protected Health Information requiring specific written Individual consent for disclosure under Applicable Law. An Individual who is onboarded as opted in will be included in ILHIE Connect unless and until the Individual affirmatively opts out in accordance with the procedures set forth herein.
- 2.0 Meaningful Disclosure.** To ensure that an Individual is able to make meaningful and informed choices about his or her participation in ILHIE Connect, each Individual will be offered the ILHIE Notice at the point of care at each Individual's first encounter with a Participant after it contracts to become a Participant, or, in the event of a medical emergency that makes it impossible to offer the ILHIE Notice to the Individual at the first encounter, as soon thereafter as is practicable, and to Active Patients on an annual basis thereafter.
- 3.0 ILHIE Connect Participation.** If an Individual is opted in to ILHIE Connect, a summary of his or her health information will be disclosed in response to a specific request, made by a Participant for a Permitted Purpose. However, an Individual's Protected Health Information will not be disclosed in response to such a request

when it contains Specially Protected Health Information unless consent authorizing that Participant to disclose such Specially Protected Health Information through ILHIE Connect has been given by the Individual to the Participant that holds such data.

- 3.1** An Individual who does not want his or her health information to be disclosed to other Participants may opt out by following the procedures below. If an Individual does opt out, the Individual's Protected Health Information will not be disclosed through the ILHIE for any purpose except as required or permitted by Applicable Law.
 - 3.2** An Individual may decide at any time to change his or her preference to opt out or opt in to ILHIE Connect, including the revocation of a prior election to opt out of participation in ILHIE Connect.
 - 3.3** An Individual's ILHIE Connect participation is specific to each Participant that maintains Protected Health Information about that Individual. An Individual who desires to opt out of ILHIE Connect participation on a State-wide basis must opt-out with each of the Individual's health care providers who are Participants. Alternatively, an Individual can choose to participate in ILHIE Connect on a Participant-by-Participant basis.
- 4.0 Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
- 4.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures

Patient and Participant Procedures

- 1.0** After a Participant contracts to join ILHIE Connect, that Participant must present the ILHIE Notice (i) at the point of care to each Individual at the Individual's first encounter with that Participant, or, in the event of a medical emergency that makes it impossible to offer the ILHIE Notice to the Individual at the first encounter, as soon thereafter as is practicable; and (ii) to each Active Patient, on an annual basis thereafter. In the sole discretion of the Participant, the Participant may offer the ILHIE Notice to an Individual by any reasonably appropriate means, including but not limited to by mail, email, or Individual portal. Participants are encouraged to post a copy of the ILHIE Notice on the Participant's own website, if any, and to record the presentation of the ILHIE Notice in the Individual's medical record.
- 2.0** The Participant must prominently and consistently display the ILHIE Signage.
- 3.0** The Participant may display and make available any other materials about ILHIE Connect that are developed, approved and made freely available by the ILHIE

Authority to Participants in a public area of the Participant's office or facility, on the Participant's website, or both.

- 4.0** Participant may amend its current Notice of Privacy Practices ("NPP") to reflect its contemplated requests, uses, and disclosure of Protected Health Information through the ILHIE; however, amendment of a Participant's NPP will not satisfy ILHIE meaningful disclosure requirements. The ILHIE Notice is separate and apart from any requirements the Participant is obligated to comply with pursuant to HIPAA or the Participant's HIPAA NPP.
- 5.0** If an Individual asks questions about ILHIE Connect, the Participant or Participant's designee (e.g. HIPAA Privacy Officer) will respond to the Individual, including responding to questions about the contents of the ILHIE Notice, including the potential benefits and risks of participation in ILHIE Connect.
- 6.0** No action is needed by an Individual who is a patient of a Participant if that Individual wishes to participate in ILHIE Connect and the Individual does not have Specially Protected Health Information in his or her medical record. An Individual shall participate in ILHIE Connect unless and until the Individual elects not to participate through proper completion of the Opt-Out Form. If the Individual does not want to share his or her Protected Health Information held by a specific Participant, an Individual must submit an Opt-Out Form to each such Participant whose data the Individual does not wish to have shared.
- 7.0** An Individual may elect to not participate in ILHIE Connect at any time by executing an Opt-Out Form. A Participant must allow an Individual to opt out of ILHIE Connect participation at any time, even after having already been enrolled in ILHIE Connect; however, any exchange of Protected Health Information that may have occurred prior to an Individual's decision to opt-out will not be reversed.
- 8.0** If an Individual elects to opt out of ILHIE Connect at the point of care, and the Individual's identity has been collected by the Participant, the Participant will require the Individual to document his or her decision to opt out by utilizing the Opt-Out Form. A copy of this signed Opt-Out Form will be kept and maintained by the receiving Participant in the Individual's medical record in accordance with the Participant's policies and Applicable Law governing health record retention. If the Individual who is participating in ILHIE Connect fails or refuses to sign an Opt-Out Form at the point of care, the Participant will inform the Individual that the Individual will continue to participate in ILHIE Connect unless the Opt-Out Form is properly completed.
- 9.0** An Individual may elect to opt out of ILHIE Connect by either of the following means:

 - (i) Completing and submitting the Opt-Out Form to the Individual's Participant during an Individual's encounter with the Participant, or
 - (ii) Obtaining the Opt-Out Form from the ILHIE Authority website and submitting the completed, notarized form to the ILHIE Authority by U.S. mail, facsimile, or as a scanned attachment to an email.

- 10.0** If requested, a Participant will assist the Individual to opt in to participation in ILHIE Connect after not participating. The Participant will supply the Individual with the Opt-In Form. An Individual may elect to opt in to ILHIE Connect after not participating by completing and submitting the Opt-In Form to the Individual's Participant during an Individual's encounter with the Participant, and providing any appropriate consent. After an Individual has not participated in ILHIE Connect with respect to a specific Participant(s), an Individual must submit an Opt-In Form to each such Participant(s) that the Individual wishes to share the Participant's data about the Individual through ILHIE Connect.
- 11.0** If an Individual elects to opt in to ILHIE Connect at the point of care, and the Participant obtains the requisite written consent for disclosure of Specially Protected Health Information, a copy of the signed Opt-In Form and requisite written consent will be maintained by the receiving Participant in the Individual's medical record in accordance with the Participant's policies and Applicable Law governing health record retention. If the Individual who is requesting to participate in ILHIE Connect fails or refuses to sign an Opt-In Form and requisite written consent for disclosure of Specially Protected Health Information at the point of care, the Participant will inform the Individual that the Individual will not participate in ILHIE Connect for that specific Participant unless the forms are properly completed.
- 12.0** If Participant's EHR can ensure that Specially Protected Health Information will not be made available through ILHIE Connect, then the Participant must ensure that the Participant's EHR does not make Specially Protected Health Information available through ILHIE Connect unless an Individual with Specially Protected Health Information has given consent to the disclosure of the information to that Participant. If Participant's EHR cannot ensure that an Individual's Specially Protected Health Information will not be made available through ILHIE Connect, then the Participant must either (i) obtain the Individual's consent to disclose the Specially Protected Health Information, or (ii) make the Individual's entire medical record unavailable through ILHIE Connect by on-boarding the Individual as opted-out.
- 13.0** A minor Individual aged 12 years old or older has the capacity to consent to ILHIE Connect participation to the same extent as a person of legal age. A Participant will comply with the ILHIE Connect participation decision made by a parent or legal guardian for his or her minor child aged 11 or under. If deemed necessary by the Participant, a parent or legal guardian may be required to present the Participant with proof of legal guardianship or other legal authority to act on behalf of a minor child aged 11 or under.
- 14.0** Upon reaching age 12, a minor Individual whose participation decision was previously expressed by his or her parent or legal guardian must be given the opportunity to exercise his or her own participation decision in accordance with the procedures outlined in Sections 1 through 13 above.
- 15.0** Upon on-boarding to ILHIE Connect, each Participant will electronically supply the ILHIE Authority with personal demographic information about all of the Individuals who are patients of Participant so that Other Participants may request the Protected

Health Information of Individuals who are patients of the Participant through ILHIE Connect, if available, for Permitted Purposes.

- 16.0** All elections to opt out of ILHIE Connect or to opt in to ILHIE Connect made by Individuals at the point of care will be electronically communicated by the Participant to the ILHIE Authority within one (1) business day of receipt or as required by contract, but in no event should communication take longer than three (3) business days.
- 17.0** Participant shall not deny care to any Individual because he or she elects to participate in, or opt out of, ILHIE Connect.

ILHIE Authority Procedures

- 1.0** The ILHIE Authority will develop, approve, and make freely available on its website the ILHIE Notice, which may be updated from time to time.
- 2.0** The ILHIE Authority will develop, approve, and make freely available on its website the ILHIE Signage, which may be updated from time to time.
- 3.0** The ILHIE Authority will develop, approve, and make freely available an Opt-Out Form, an Opt-In Form, and additional materials and resources for use and display by Participants in offering Individuals meaningful disclosure about ILHIE Connect and an Individual's right to opt-out of ILHIE Connect.
- 4.0** Once an Opt-In Form has been executed by the Individual and communicated to the ILHIE Authority by a Participant, the Individual will participate in ILHIE Connect, with respect to that disclosing Participant, from the date the ILHIE Authority processes the Opt-In request. All Individual ILHIE Connect participation elections which are provided to the ILHIE Authority electronically will be immediately and electronically recorded by the ILHIE Authority to ensure compliance with each Individual's decision.
- 5.0** An Individual's election to opt out through submission of a complete, notarized Opt-Out Form directly to the ILHIE Authority will be implemented by the ILHIE Authority as soon after receipt as practicable, but in no event longer than three (3) business days.
- 6.0** Upon on-boarding to ILHIE Connect, the Participant will electronically supply the ILHIE Authority with personal demographic information about all of the Individuals that are patients of the Participant. The ILHIE Authority will electronically maintain personal demographic information about Individuals that are patients of each Participant in a Master Patient Index. The ILHIE Authority will also use the Master Patient Index to record and maintain each Individual's ILHIE Connect participation decision with respect to that Participant. The last participation decision received by the ILHIE Authority will govern the Individual's consent preference with respect to that Participant. The ILHIE Authority will utilize Individual personal demographic information to enable Other Participants to access the health information of Individuals for Permitted Purposes.

- 7.0** For an Individual who is participating in ILHIE Connect with one or more Participants, the ILHIE Authority will share a summary of all of an Individual's Protected Health Information that is available through ILHIE Connect in response to a query from any Participant.
- 8.0** For an Individual who has opted out of ILHIE Connect with one or more Participants, the ILHIE Authority will not allow disclosure of Protected Health Information from those Participant(s) for any purpose except as permitted by Applicable Law, such as public health reporting. Instead, a message will be sent to the requesting Participant to the effect that there is "no information available."
- 9.0** The ILHIE Authority will provide outreach, educational information and, where requested, technical assistance to Individuals and Participants to promote the consistent implementation of the participation procedures outlined in this Policy and Procedure.

Associated Policies and References:

740 ILCS 110

Request, Use, and Disclosure of Protected Health Information

Emergency Access

Enforcement

Information Subject to Special Protection

Sanctions

Definitions

Applicable Law

EHR

ILHIE Connect

ILHIE Notice

ILHIE Signage

Individual

Master Patient Index

Opt-Out Form

Opt-In Form

Participant

Permitted Purposes

Policies and Procedures

Protected Health Information

Specially Protected Health Information

| |
|--|
| Policies and Procedures |
| POLICY: Information Subject to Special Protection |
| Policy #7 |
| Effective Date: April 2, 2014 |

Purpose: This policy describes the handling of Specially Protected Health Information. Specially Protected Health Information may not be disclosed to or through the ILHIE without written Individual consent for disclosure that complies with Applicable Law. The policy also describes the categories of Specially Protected Health Information that must be disclosed through some means other than ILHIE Connect.

The ILHIE Authority is committed to protecting and respecting the privacy of Individual's Protected Health Information, and especially Specially Protected Health Information that may be particularly sensitive.

Policy:

1.0 Individual Consent for Disclosure of Specially Protected Health Information.

Federal and Illinois laws protect against the disclosure of certain categories of Protected Health Information that may be considered particularly private or sensitive to an Individual, unless the Individual consents to the disclosure. An Individual's Specially Protected Health Information may not be disclosed through the ILHIE unless the disclosure is consistent with these Policies and Procedures, in particular the Patient Choice and Meaningful Disclosure Policy (Policy #6), the Data Sharing Agreement, and Applicable Law.

- 1.1** Participants may not disclose to or through ILHIE Connect any Specially Protected Health Information for which the Participant does not have the appropriate Individual consent to disclose.
- 1.2** Participants shall not disclose through ILHIE Connect any Protected Health Information, including Specially Protected Health Information, protected by 42 C.F.R Part 2.
- 1.3** Any good or service for which an Individual has paid out-of pocket in full, and for which the Individual has requested the Participant to restrict the disclosure of said goods and services to a Health Plan, shall be honored by the Participant.
- 1.4** The ILHIE Authority shall give annual consideration to technological advances that may support granular level data segmentation that increases Individual control over the further disclosure by the ILHIE or another health information exchange to third parties of selected portions of the Individual's record while permitting disclosures of the Individual's remaining Protected Health Information.
- 1.5** Any Participant who becomes aware that it has received unauthorized Protected Health Information, including Specially Protected Health Information, through the ILHIE shall immediately notify the ILHIE Authority and must return or destroy such unauthorized information.

2.0 Compliance. Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

2.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies and References:

42 C.F.R Part 2

45 C.F.R §164.522

740 ILCS 14/9.6

Access, Use and Disclosure of Protected Health Information
Enforcement

Patient Choice and Meaningful Disclosure

Sanctions

Definitions

Applicable Law

Health Plan

ILHIE Authority

Individual

Participant

Protected Health Information

Specially Protected Health Information

| |
|--------------------------------------|
| Policies and Procedures |
| POLICY: Emergency Access |
| Policy #8 |
| Effective Date: April 2, 2014 |

Purpose: This policy defines the scope of the Individual opt-out regarding the permitted disclosure of Individual Protected Health Information in the event of a medical emergency within the context of ILHIE Connect.

Policy:

- 1.0 Emergency Access.** There is no ability to “break the glass” in Illinois for those Individuals who have opted out of ILHIE Connect. The ILHIE Authority does not authorize Participant opt-out overrides (also known as “breaking the glass”) in the case of a medical emergency for an Individual who has opted out of participation in ILHIE Connect.
- 2.0 Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
 - 2.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant’s compliance with these Policies and Procedures.

Procedures:

- 1.0** The Opt-Out Form shall clearly state that Protected Health Information will not be available through ILHIE Connect, even in an emergency, for an Individual who opts out.
- 2.0** If a Participant or its Authorized User requests information through ILHIE Connect about an Individual who has opted out of ILHIE Connect in a medical emergency or in any other circumstance, a message will be sent to the querying Participant or Authorized User to the effect that there is “no information available” about that Individual.

Associated Policies and References

Enforcement

Resolution 2013-15 Recommendation on Break the Glass Policy to the Data Security and Privacy Committee of the Illinois Health Information Exchange Authority

Sanctions

Definitions

Authorized User

ILHIE Authority

ILHIE Connect

Individual

Opt-Out Form
Participant
Protected Health Information

| |
|--|
| Policies and Procedures |
| POLICY: Individual Access to Data |
| Policy #9 |
| Effective Date: April 2, 2014 |

Purpose: Pursuant to HIPAA (45 C.F.R §164.524) and Illinois law (735 ILCS 5/8-2001), Individuals generally have the right of access to inspect and obtain a copy of the Individual's Protected Health Information that is held in a Designated Record Set. This policy describes the role of the ILHIE Authority in ensuring that Individuals may seek access to their own Protected Health Information that is made available through the ILHIE.

The ILHIE is not a repository of Designated Record Sets containing Protected Health Information for or on behalf of its Participants. The ILHIE currently facilitates the secure exchange of Protected Health Information between Participants for one or more Permitted Purposes. Participants are the originators and custodians of Individual Protected Health Information and Designated Record Sets. As such, the Participant(s) who maintains a Designated Record Set for an Individual requesting access is the only entity that can evaluate the request and determine whether access may be granted.

Policy:

- 1.0 Right of Access.** Upon the ILHIE Authority's receipt of a request from an Individual for access to inspect and obtain a copy of the Individual's Protected Health Information, the Individual will be informed that the ILHIE Authority does not maintain the Designated Record Set containing the Protected Health Information and that the Individual should direct their request to the applicable Participant(s).
 - 1.1** The ILHIE Authority will not directly provide an Individual with access to his or her own Protected Health Information but will instead assist an Individual in requesting access to his or her Protected Health Information from the appropriate Participant(s).
 - 1.2** Participants shall comply with an Individual's rights to access their Protected Health Information in accordance with Applicable Law.
- 2.0 Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
 - 2.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures:

Participant Procedures

- 1.0** The applicable Participant(s) will be solely responsible for determining whether to grant or deny an Individual's request for access to Protected Health Information in compliance with Applicable Law.
- 2.0** If an Individual is determined by the applicable Participant(s) to be entitled to access some or all of the Individual's Protected Health Information, the Participant will be solely responsible for the timely provision of the required access to the Individual.
- 3.0** The applicable Participant(s) is responsible for accomplishing the provision of access of an Individual's Protected Health Information in compliance with Applicable Law, including but not limited to 45 C.F.R §164.524, its standards and implementation specifications, and the HITECH Act.

ILHIE Procedures

- 1.0** The ILHIE Authority will facilitate an Individual's request for access to the Individual's Protected Health Information by assisting in identifying to the Individual the Participant(s) who maintain the Individual's Protected Health Information in a Designated Record Set, upon request.

Associated Policies and References

42 U.S.C. §§300jj et seq.; §§17901 et seq.

45 C.F.R §164.524

735 ILCS 5/8-2001

Enforcement

Sanctions

Definitions

Applicable Law

Designated Record Set

HIPAA

ILHIE Authority

Individual

Participant

Permitted Purposes

Policies and Procedures

Protected Health Information



| |
|---|
| .Policies and Procedures |
| POLICY: Individual Amendment of Data |
| Policy #10 |
| Effective Date: April 2, 2014 |

Purpose: Pursuant to HIPAA (45 C.F.R §164.526), an Individual generally has the right to request an amendment of Protected Health Information about the Individual that is contained in the Designated Record Set of a Covered Entity. This policy describes the role of the ILHIE Authority in ensuring that Individuals may seek to amend their Protected Health Information that is made available by a Participant to and through the ILHIE.

The ILHIE is not a repository of Designated Record Sets containing Protected Health Information for or on behalf of its Participants. The ILHIE currently facilitates the secure exchange of Protected Health Information between Participants for one or more Permitted Purposes. Participants are the originators and custodians of Individuals' Protected Health Information and Designated Record Sets. As such, the Participant(s) that maintain a Designated Record Set for an Individual requesting an amendment is the only entity that can evaluate the request and determine whether the amendment may be granted. The ILHIE Authority does not have the authority or access to amend Protected Health Information originated and maintained by Participant(s).

Policy:

1.0 Right to Amend. Upon the ILHIE Authority's receipt of a request from an Individual to amend the Individual's Protected Health Information, the Individual will be informed that the ILHIE Authority does not maintain the Designated Record Set containing the Protected Health Information and that the Individual should direct their request to the applicable Participant(s).

1.1 The ILHIE Authority will not directly process an Individual's request for amendment of his or her own Protected Health Information but will instead assist Individuals in requesting the amendment from the appropriate Participant(s).

1.2 Participants shall comply with an Individual's rights to amend Protected Health Information in accordance with Applicable Law.

2.0 Informing Other Participants. If an Individual requests, and the Participant(s) accepts, an amendment to the Protected Health Information about the Individual, the Participant(s), assisted by the ILHIE Authority, if requested by Participant, that made the amendment shall make reasonable efforts to inform and provide the amendment within a reasonable time to:

- (i) Other Participant(s) identified by the Individual or the ILHIE Authority as having received Protected Health Information about the Individual and needing the amendment; and
- (ii) Other Participant(s) that the amending Participant knows have received the Protected Health Information that is the subject of the amendment and that

may have relied, or could foreseeably rely, on such information to the detriment of the Individual.

- 3.0. Amendment to Individual Patient Matching.** If a Participant discovers or if it is notified by an Individual, or another person or entity, that the Protected Health Information received in response to an ILHIE query about a specific Individual is not the Protected Health Information of the Individual queried (also known as “patient matching”), the Participant will immediately inform the ILHIE Authority. The ILHIE Authority will immediately investigate and take appropriate corrective action.
- 4.0 Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
- 4.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant’s compliance with these Policies and Procedures.

Procedures:

Participant Procedures

- 1.0.** The applicable Participant(s) will be solely responsible for determining whether to grant or deny an Individual’s request for amendment of Protected Health Information in compliance with Applicable Law.
- 2.0.** The applicable Participant(s) is responsible for accomplishing the amendment of an Individual’s Protected Health Information in compliance with Applicable Law, including but not limited to 45 C.F.R §164.526, its standards and implementation specifications.

ILHIE Procedures

- 1.0** The ILHIE Authority will facilitate Individual requests for amendment to the Individuals’ Protected Health Information by assisting in identifying to the Individual the Participant(s) who maintain the Individual’s Protected Health Information in a Designated Record Set, upon request.
- 2.0** The ILHIE Authority will cooperate in identifying to an Individual the Participant(s) that have accessed an Individual’s Protected Health Information in its pre-amendment form, upon request.

Associated Policies and References:

45 C.F.R §164.526

Enforcement

Information Systems Activity Review

Sanctions

Definitions

Applicable Law

Covered Entity

Designated Record Set

Individual

Participants

Permitted Purpose

Protected Health Information

| |
|---|
| Policies and Procedures |
| POLICY: Individual Accounting of Disclosures |
| Policy #11 |
| Effective Date: April 2, 2014 |

Purpose: Pursuant to HIPAA (45 C.F.R §164.528), Individuals have the right to an accounting of disclosures of the Individual's Protected Health Information made by a Covered Entity, with certain exceptions. This policy describes the ILHIE Authority and each Participant's responsibility as it relates to facilitating an Individual's ability to obtain information regarding the disclosure of the Individual's Protected Health Information.

The HITECH Act extends an Individual's right to an accounting to include disclosures to carry out Treatment, Payment, and Health Care Operations through an EHR. This policy will be reconsidered and revised in accordance with anticipated federal regulations related to this right once they become final.

Policy:

1.0 Right to an Accounting of Disclosures. Participants are required by Applicable Law to make available an accounting of certain disclosures of an Individual's Protected Health Information.

1.1 Individual requests received by the ILHIE Authority for an accounting of disclosures of the Individual's Protected Health Information will be forwarded to applicable Participant(s), unless the Individual requests an accounting of disclosures specific only to the Individual's Protected Health Information disclosed through the ILHIE.

1.2 The ILHIE Authority shall record all disclosures of Individual Protected Health Information by each Participant made through the ILHIE.

2.0 Compliance. Participants shall comply with these Policies and Procedures. The ILHIE Authority shall monitor and enforce compliance with and adherence to these Policies and Procedures.

2.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures:

Patient Procedures

1.0 Individuals are encouraged to direct requests for an accounting of disclosures of the Individual's Protected Health Information to the applicable Participant(s), unless the Individual is requesting an accounting of disclosures specific only to the Individual's Protected Health Information disclosed through the ILHIE. Individuals may submit in

writing, on a form developed and approved by the ILHIE Authority or through other appropriate means, a request for an accounting of disclosures directly to the ILHIE Authority.

Participant Procedures

- 1.0** Participants disclosing Protected Health Information through the ILHIE shall implement a system to record such information as may be necessary to meet its obligations to provide Individuals with an accounting of disclosures of Protected Health Information under Applicable Law.
- 2.0** The applicable Participant(s) shall be responsible for evaluating each Individual request for an accounting of disclosures, determining whether an accounting will be made to the Individual and providing an accounting if appropriate, in compliance with Applicable Law.
- 3.0** The applicable Participant(s) may request the ILHIE Authority to provide the Participant with an accounting of disclosures of an Individual's Protected Health Information made through the ILHIE to enable the Participant to respond to a request for an accounting by an Individual.

ILHIE Authority Procedures:

- 1.0** The ILHIE Authority shall facilitate Individual requests for an accounting of the Individual's Protected Health Information received directly by the ILHIE Authority by forwarding the request to the applicable Participant(s) within ten (10) business days of receipt. The ILHIE Authority will thereafter notify the Individual that the request was forwarded, and will identify to the Individual the Participant(s) to which the request was directed. If requested, the ILHIE Authority will provide an Individual an accounting of disclosures specific only to the Individual's Protected Health Information disclosed through the ILHIE.
- 2.0** In response to an Individual or Participant inquiry regarding requests and disclosures of an Individual's Protected Health Information through the ILHIE, the ILHIE Authority will offer to make available audit log segments relevant to the Individual's Protected Health Information that is the subject of the request.
- 3.0** The ILHIE Authority shall ensure that the ILHIE Authority is capable of tracking all disclosures of Individual Protected Health Information by each Participant made through the ILHIE. The information tracked for each disclosure shall be sufficient to enable a Participant and the ILHIE Authority to provide an accounting to an Individual that complies with all Applicable Law.
- 4.0** The ILHIE Authority shall respond to Individual requests for an accounting of disclosures specific only to the Individual's Protected Health Information disclosed through the ILHIE within 60 days, with a maximum of one 30 day extension, from the ILHIE Authority's receipt of such request. For each disclosure for which an accounting must be provided, the ILHIE Authority response shall at a minimum include the following information:

- (i) The date of the disclosure;
- (ii) The name of the Participant that received the Protected Health Information and, if known, the address of such Participant;
- (iii) A brief description of the Protected Health Information disclosed; and
- (iv) A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the written request for the disclosure as made under Applicable Law.

5.0 The ILHIE Authority shall respond to a written request from a Participant for an accounting of disclosures of an Individual's Protected Health Information through the ILHIE where the Individual is a patient of that Participant within 45 days of the ILHIE Authority's receipt of the request, unless the Participant agrees to an extension. For each disclosure for which an accounting is requested, the ILHIE Authority will make reasonable efforts to provide information sufficient to enable the Participant to provide an accounting to the Individual that complies with Applicable Law.

6.0 The ILHIE Authority shall not charge an Individual, or a Participant on behalf of an Individual, a fee for the first request for an accounting within a calendar year; however, the ILHIE Authority may charge a reasonable, cost-based fee for each subsequent request for an accounting by the same Individual or Participant upon behalf of the same Individual within the 12 month period, in a manner consistent with Applicable Law. If a fee will be required, the ILHIE Authority shall inform the Individual or Participant prior to processing the request.

7.0 The ILHIE Authority shall make an accounting of disclosures and audit log segments relevant to a requesting Individual's own data available for six (6) years or otherwise consistent with Applicable Law.

Associated Policies and References

42 U.S.C. §13405(c)

45 C.F.R §164.528

Enforcement

Information Systems Activity Review

Sanctions

Definitions

Applicable Law

Business Associate

EHR

Health Care Operations

HITECH Act

ILHIE Authority

Individual

Participant

Payment

Protected Health Information

Treatment

Purpose: This policy establishes the minimum necessary standard for requesting, using, and disclosing Protected Health Information through the ILHIE. Participants cannot request, use or disclose Protected Health Information through the ILHIE other than for Permitted Purposes.

Policy:

- 1.0 Minimum Necessary.** Consistent with HIPAA, Participants and the ILHIE Authority, when it is a Business Associate to Participants, shall make reasonable efforts to request, use and disclose only the minimum necessary Protected Health Information through the ILHIE to accomplish the Permitted Purpose for which such Protected Health Information is requested, used or disclosed.
 - 1.1** Each Participant shall develop and maintain appropriate written policies and procedures to limit unnecessary or inappropriate requests, use and disclosure of Protected Health Information through the ILHIE by the Participant's Authorized Users and to limit requests, uses and disclosures of Protected Health Information through the ILHIE to only the minimum necessary needed by such Authorized Users to perform their job functions or duties consistent with the Participant's Authorized User access control policy.
- 2.0 Treatment Exception.** The minimum necessary obligations set forth in this Policy and Procedure do not apply to the request, use, or disclosure of Protected Health Information by a Participant for Treatment purposes as defined under HIPAA, including but not limited to the coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to an Individual, or the referral of an Individual for health care from one health care provider to another.
- 3.0 Disclosures.** A Participant may rely on the scope of an Other Participant's request for Protected Health Information as being consistent with the Other Participant's minimum necessary policy and Applicable Law.
- 4.0 Application to Health Plans.** A Participant that is a health plan shall access and use Protected Health Information of Another Participant only for Payment purposes as defined under HIPAA.
 - 4.1** Participants that are health plans shall request and use only the minimum necessary Protected Health Information when using information for Payment purposes.

5.0 Compliance. Participant shall comply with these Policies and Procedures. The ILHIE Authority shall monitor and enforce compliance with and adherence to these Policies and Procedures.

5.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies and References:

45 C.F.R §164.502(b)

45 C.F.R §164.514(d)

Data Sharing Agreement

Enforcement

Sanctions

User Authorization

Definitions

Authorized Users

Health Care Provider

HIPAA

Participants

Payment

Permitted Purposes

Protected Health Information

Minimum Necessary

Treatment



| |
|--|
| Policies and Procedures |
| POLICY: ILHIE Authority Workforce, Agents, Contractors and Subcontractors |
| Policy #13 |
| Effective Date: April 2, 2014 |

Purpose: This policy sets forth the responsibilities and terms under which the ILHIE Authority and its Workforce, contractors, Subcontractors, and agents may request, use or disclose Protected Health Information created, received, maintained, or transmitted using the ILHIE.

Policy:

- 1.0 Authorized Purposes.** The ILHIE Authority may authorize its Workforce, contractors, Subcontractors, and agents to request, use, or disclose Protected Health Information set forth in the Request, Use, and Disclosure of Protected Health Information Policy (Policy #5), the Data Sharing Agreement, and other applicable contracts, in accordance with the Minimum Necessary Policy (Policy #12) and only as permitted by Applicable Law.
- 2.0 Authorized Users.** The ILHIE Authority shall implement policies and procedures reasonably designed to enable members of its Workforce, contractors, Subcontractors and agents to disclose, in accordance with the role and job responsibility of the individual, only such Protected Health Information as is reasonably required to accomplish the performance of the purpose for which the Protected Health Information is being accessed or used.
- 3.0 Training.** ILHIE Authority Workforce members, contractors, Subcontractors, and agents may not access Protected Health Information through the ILHIE unless such individual has received training regarding these Policies and Procedures and the Workforce member's, contractors', Subcontractors', and agent's obligations under Applicable Law, and has acknowledged in writing the receipt of such training.
- 4.0 Compliance.** The ILHIE Authority shall discipline Workforce members, contractors, Subcontractors, and agents who are not in compliance with these Policies and Procedures or engage in any other unauthorized or inappropriate behavior that undermines the privacy or security of Protected Health Information created, received, maintained or transmitted through the ILHIE. Depending on the circumstances, disciplinary measures may include verbal and written warnings, retraining, demotion, suspension or termination of employment.
 - 4.1** The ILHIE Authority shall require all of its Workforce members, contractors, Subcontractors, and agents to report any actual or suspected non-compliance with these Policies and Procedures, the Data Sharing Agreement or Applicable Law of which they become aware. No Workforce member, contractor, Subcontractor, or agent may be subject to retaliation of any kind for reporting an actual or suspected non-compliance in good faith.
 - 4.2** Participants shall comply with these Policies and Procedures.

- 4.3** The ILHIE Authority shall monitor and enforce compliance with and adherence to these Policies and Procedures.
- 4.4** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies & Procedures

45 C.F.R §160.103

45 C.F.R §160.514(a)-(c)

Data Sharing Agreement

Enforcement

ILHIE Personnel Handbook

Sanctions

Definitions

Authorized User

Subcontractor

Workforce

| |
|--|
| Policies and Procedures |
| POLICY: Complaint Handling and Resolution |
| Policy #14 |
| Effective Date: April 2, 2014 |

Purpose: This policy establishes a process by which anyone who suspects there has been an incident of non-compliance with respect to the privacy or security of Protected Health Information requested, used or disclosed through the ILHIE may report the suspected incident. This policy also establishes ILHIE Authority requirements for reviewing and resolving such complaints in a timely manner.

Policy:

- 1.0 Right to File a Complaint.** Any person or entity, including but not limited to an Individual, Participant, or Authorized User, who desires to file a complaint ("Complaining Party") with the ILHIE Authority to report a potential incident of non-compliance with respect to the privacy or security of Protected Health Information requested, used, or disclosed through the ILHIE may do so in writing, utilizing a form developed and approved by the ILHIE Authority, or by other appropriate means.
 - 1.1** All complaints will be directed to the ILHIE Privacy and Compliance Officer ("PCO") for handling.
 - 1.2** Complaints may be made on an anonymous basis.
 - 1.3** Neither the ILHIE Authority nor Participants shall threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against a Complaining Party.
- 2.0 Investigation.** Upon receipt of a complaint, the ILHIE PCO will acknowledge the complaint to the Complaining Party, if known.
 - 2.1** The ILHIE PCO shall initiate a review of the complaint upon receipt. After completion of the review, an investigation of the complaint will be initiated if, in the discretion of the ILHIE PCO, an investigation is warranted. The ILHIE PCO shall consult appropriate ILHIE Authority staff and other individuals when conducting reviews and investigations.
 - 2.2** If warranted, the ILHIE Authority may request that a Participant undertake its own review or investigation. The Participant shall keep the ILHIE Authority informed of the progress of such review or investigation upon reasonable request; however, the ILHIE Authority will not participate in or seek information regarding any review or investigation by a Participant that could result in the loss of any applicable attorney-client privilege or work product protections.
- 3.0 Cooperation.** A Participant shall reasonably cooperate and, upon reasonable request, make Participant personnel, policies, procedures, and practices available or

known to the ILHIE Authority, including the ILHIE PCO, when the ILHIE Authority undertakes a review and/or an investigation related to a complaint filed with the ILHIE Authority.

4.0 Resolution. The Complaining Party, if known, shall be notified in writing of the results of a review or investigation by the ILHIE Authority.

4.1 If a complaint is verified, the ILHIE Authority, shall, as recommended, develop and implement appropriate corrective measures. Participants shall implement corrective measures at the reasonable request of the ILHIE Authority.

4.2 Any Complaining Party not satisfied by the ILHIE Authority's proposed resolution of a complaint may request that ILHIE Authority reconsider the matter.

4.3 Upon reasonable request, a Participant shall inform the ILHIE Authority of progress towards implementing corrective measures; however, the ILHIE Authority need not be notified of specific workforce disciplinary actions.

5.0 Compliance. Participants shall comply with these Policies and Procedures. The ILHIE Authority shall monitor and enforce compliance with and adherence to these Policies and Procedures.

5.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures:

Complaining Party Procedures

1.0 A Complaining Party may submit a complaint to the ILHIE PCO in any manner, including but not limited to:

- (i) In writing, on either a Complaint Form developed and approved by the ILHIE Authority, or in a separate writing that includes the information set forth under ILHIE Authority procedures 1.0;
- (ii) By electronic mail, to the ILHIE PCO at ILHIE.Privacy@illinois.gov; or
- (iii) By phone, at (312) 814-1255.

2.0 If the Complaining Party is identified in the complaint, the Complaining Party may request that the ILHIE Authority maintain the confidentiality of the identity of the Complaining Party. The ILHIE Authority shall respect this request for confidentiality unless, by doing so, the Complaining Party or another person would be placed at significant risk or disclosure is otherwise required by Applicable Law.

3.0 If a Complaining Party is not satisfied by the ILHIE Authority's proposed resolution of a complaint, then the Complaining Party may request that ILHIE Authority reconsider the matter.

ILHIE Authority Procedures

- 1.0** The ILHIE Authority shall develop and approve a Complaint Form. The Complaint Form will request, at a minimum, the following:
 - (i) The name of the party that is the subject of the complaint, if known; and
 - (ii) A description of the acts or omissions believed to be in non-compliance with respect to the privacy or security of Protected Health Information requested, used, or disclosed through the ILHIE.
- 2.0** The ILHIE Authority will provide information on its website about the right of persons including Individuals, Participants, and Authorized Users, to file a complaint, including a copy of the approved Complaint Form.
- 3.0** Within five (5) business days of receiving a complaint, the ILHIE PCO shall:
 - (i) Acknowledge receipt of the complaint to the Complaining Party, if the Complaining Party is known;
 - (ii) Forward a de-identified summary of the complaint to the named Participant(s), if applicable; and
 - (iii) Initiate the review and, if determined warranted, investigation of the complaint.
- 4.0** Upon request, the ILHIE Authority will respect any request for confidentiality made by the Complaining Party unless, by doing so, the Complaining Party or any other person would be placed at significant risk or disclosure is otherwise required by Applicable Law.
- 5.0** The ILHIE Authority shall make reasonable efforts to review and, if necessary, investigate and resolve complaints, provide feedback to the Complaining Party, and implement corrective measures within thirty (30) days of receiving the complaint.
 - 5.1** If necessary, the ILHIE PCO may extend this deadline in his or her sole discretion as necessary, so long as notice explaining a reason for the delay is provided to the Complaining Party, if known, prior to the thirty (30) day deadline.
- 6.0** If, after review, a complaint of non-compliance cannot be verified, then no further action by the ILHIE Authority, including the ILHIE PCO, shall be required other than to notify the Complaining Party, if known, that the complaint could not be verified.
- 7.0** If a complaint of non-compliance is verified, then the ILHIE Authority shall determine appropriate actions including but not limited to corrective measures to seek to resolve the root cause of complaint.
 - 7.1** The ILHIE PCO shall notify the Complaining Party, if known, of the ILHIE Authority's response to the complaint in writing.

- 7.2** The ILHIE PCO shall notify the non-compliant Participant(s) in writing of the actions that the ILHIE PCO has determined to be appropriate to seek to resolve the root cause of the complaint, which may include a corrective action plan.
- 7.3** Any complaints involving a potential Breach of Protected Health Information shall trigger implementation of the Breach Notification and Mitigation Policy (Policy #21).
- 8.0** The ILHIE Authority shall maintain copies of all written Complaint Forms for at least six (6) years from receipt.
- 9.0** The ILHIE Authority shall review all filed complaints to determine if persistent or recurrent problems exist within the ILHIE or ILHIE Authority operations on a regular basis.
- 10.0** The ILHIE Authority shall provide a summary of the findings related to complaints to the ILHIE Authority Data Security and Privacy Committee on at least an annual basis.

Associated Policies & Procedures

45 C.F.R §164.306

Breach Notification and Mitigation Policy

Enforcement

Information Systems Activity Review

Sanctions

Definitions

Authorized User

Complaint Form

Individual

Participant

| |
|--------------------------------------|
| Policies and Procedures |
| POLICY: Sanctions |
| Policy #15 |
| Effective Date: April 2, 2014 |

Purpose: This policy defines the circumstances under which participation in the ILHIE by a Participant or Authorized User may be revoked, suspended or reinstated.

Policy:

1.0 Revocation or Suspension of Authorized User Access. The ILHIE Authority or a Participant may immediately revoke or suspend its respective Authorized User's access to the ILHIE upon a determination of the Authorized User's material non-compliance with these Policies and Procedures, the Data Sharing Agreement or Applicable Law. The ILHIE Authority may immediately revoke or suspend a Participant's Authorized User's access to the ILHIE upon a determination of the Authorized User's material non-compliance with these Policies and Procedures, the Data Sharing Agreement, or Applicable Law.

1.1 In determining whether an Authorized User's access should be revoked or suspended, the ILHIE Authority or a Participant may consider any relevant factors including whether there is a substantial likelihood that an Authorized User's acts or omissions create an immediate threat or will cause irreparable harm to another party, including but not limited to an Individual whose Protected Health Information is requested, used, or disclosed through the ILHIE, the Participant, Other Participant(s), another Authorized User or the ILHIE Authority. The ILHIE Authority may additionally consider other factors including but not limited to the privacy of Individuals whose Protected Health Information is requested, used or disclosed through the ILHIE, the security of the ILHIE, the Authorized User's involvement in or response to a Breach, misuse of the Authorized User's ILHIE access, or the criminal conviction or charge of the Authorized User.

1.2 The ILHIE Authority and each Participant shall immediately revoke its respective Authorized User's access to the ILHIE, if the Authorized User ceases to be qualified as such, including but not limited to, upon termination of the Authorized User's affiliation with the ILHIE Authority or the Participant.

2.0 Participant Access, Revocation, or Suspension. The ILHIE Authority may revoke or suspend a Participant's access to the ILHIE provided that the requirements for such revocation or suspension have been met as specified in these Policies and Procedures or the Data Sharing Agreement.

2.1 Consistent with the terms of the Data Sharing Agreement, the ILHIE Authority may immediately revoke or suspend a Participant's access to the ILHIE if the ILHIE Authority reasonably believes that the Participant has suffered a Breach or is in material noncompliance with these Policies and Procedures, the Data Sharing Agreement or Applicable Law, including without limitation

the Participant or its Authorized User(s), requesting, using or disclosing or attempting to request, use or disclose Protected Health Information for other than a Permitted Purpose or in an unauthorized manner.

- 2.3** In determining whether a Participant's access should be revoked or suspended, the ILHIE Authority may consider any relevant factors including whether there is a substantial likelihood that the Participant's acts or omissions create an immediate threat or will cause irreparable harm to another party, including, but not limited to, an Individual whose health information is requested, used, or disclosed through the ILHIE, Another Participant, an Authorized User, or the ILHIE Authority. The ILHIE Authority may additionally consider other factors including but not limited to the Participant's involvement in or response to a Breach, misuse of the Participant's ILHIE access, or criminal conviction or charge.
- 2.4** The ILHIE Authority may terminate a Data Sharing Agreement with a Participant in accordance with the terms of the Data Sharing Agreement. Upon termination of a Data Sharing Agreement the terminated party shall cease to be a Participant and neither it nor its Authorized Users shall have any rights to use the ILHIE, unless the Authorized Users have an independent right to access the ILHIE through another Participant.
- 3.0 Breach.** The ILHIE Authority may revoke or suspend the ILHIE access of a Participant or its Authorized User(s) in the event of Breach or suspected Breach if the ILHIE Authority determines, in its sole discretion, that doing so is necessary to protect the privacy of Individuals or the security of the ILHIE, the ILHIE's integrity, or the availability of the network to Other Participants.
- 4.0 Authorized User Reinstatement.** The ILHIE Authority may, in its sole discretion, reinstate a Participant's Authorized User's ILHIE access where such access was revoked or suspended by the ILHIE Authority, provided that the Authorized User, in cooperation with the relevant Participant, where appropriate, has demonstrated to the ILHIE Authority's satisfaction that the Authorized User has taken necessary steps to resolve the issue resulting in the revocation or suspension.
- 4.1** A Participant may, at its own discretion, and in accordance with its own policies and procedures, reinstate the ILHIE access of one of the Participant's Authorized Users after the Participant revoked or suspended such Authorized User's access, provided that the Authorized User has demonstrated to the Participant's satisfaction that the Authorized User has taken necessary steps to resolve the issue resulting in the revocation or suspension.
- 5.0 Participant Reinstatement.** In accordance with the terms of the Data Sharing Agreement, the ILHIE Authority may, in its own discretion, reinstate a Participant's ILHIE access where such access was suspended by the ILHIE Authority, provided that the Participant, in cooperation with the ILHIE Authority, has demonstrated to the ILHIE Authority's satisfaction that the Participant has taken necessary steps to resolve the issue resulting in the revocation or suspension. A Participant may

request that the ILHIE Authority's decision to suspend its access to the ILHIE be reconsidered, in accordance with the terms of the Data Sharing Agreement.

5.1 Upon revocation of a Participant's access to the ILHIE, the Participant's Data Sharing Agreement is terminated. However, nothing shall prevent the Participant from seeking to enter a new Data Sharing Agreement with the ILHIE Authority.

6.0 **Cooperation.** Participants shall cooperate in good faith in any investigations conducted by the ILHIE Authority, including any obligations pursuant to the Breach Notification and Mitigation Policy (Policy #21).

6.1 Participants and the ILHIE Authority shall cooperate in good faith in an investigation conducted by Other Participant(s).

7.0 **Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

7.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures:

Participant Procedures

1.0 Each Participant must promptly, but in no event more than three (3) days after taking action, notify the ILHIE Authority of any action revoking or suspending the ILHIE access of its Authorized User(s).

2.0 A Participant is responsible for the Participant's Authorized Users and shall take necessary steps to resolve any issue resulting in revocation or suspension of an Authorized User in accordance with these Policies and Procedures and the Data Sharing Agreement, including but not limited to the Breach Notification and Mitigation Policy (Policy #21), and the Participant's own policies and procedures.

3.0 The Participant, in cooperation with the ILHIE Authority, shall take necessary steps to resolve the issue resulting in the revocation or suspension of the Participant or a Participant's Authorized User in accordance with these Policies and Procedures and the Data Sharing Agreement.

ILHIE Authority Procedures

1.0 The ILHIE Authority shall immediately upon revoking or suspending a Participant's access to the ILHIE, or revoking or suspending a Participant's Authorized User's access to the ILHIE, provide notice of the revocation or suspension and provide a written summary of the reasons of the same to the affected Participant. In the case

of revocation of a Participant's access, the revocation shall be handled in accordance with the terms of the Data Sharing Agreement.

- 2.0** The ILHIE Authority, in cooperation with the Participant, shall take necessary steps to resolve the issue resulting in the revocation or suspension of a Participant or a Participant's Authorized User in accordance with these Policies and Procedures and the Data Sharing Agreement.
- 3.0** All Master Patient Index data contributed to the ILHIE Authority by a revoked or suspended Participant, and audit log data pertaining to a revoked or suspended Participant's, or revoked or suspended Authorized User's, activity, shall be preserved by the ILHIE Authority to ensure its ability to conduct and respond to, or to assist Participants in conducting and responding to, appropriate Individual inquires, audits, investigations, claims, lawsuits and other authorized requests.

Associated Policies and References

Breach Notification and Mitigation Policy
Data Sharing Agreement
Enforcement
Sanctions
User Authorization

Definitions

Applicable Law
Authorized User
Data Sharing Agreement
ILHIE Authority
Master Patient Index
Participant

| |
|--------------------------------------|
| Policies and Procedures |
| POLICY: Enforcement |
| Policy #16 |
| Effective Date: April 2, 2014 |

Purpose: The ILHIE Authority has the responsibility to appropriately monitor compliance with these Policies and Procedures and the Data Sharing Agreement to build and maintain trust in and the integrity of the ILHIE. In the event that monitoring reveals a Participant's possible noncompliance with these Policies and Procedures or the Data Sharing Agreement, the ILHIE Authority will seek to correct the noncompliance, mitigate the consequences, and take appropriate corrective action, including implementing appropriate sanctions.

Policy: In accordance with these Policies and Procedures, the Data Sharing Agreement and Applicable Law, the ILHIE Authority is authorized to take an enforcement action against a Participant or its Authorized User where there is reasonable basis to believe that the Participant or its Authorized User is not in compliance with these Policies and Procedures, the Data Sharing Agreement, or Applicable Law.

- 1.0 Audit.** The ILHIE Authority, or its authorized designee, may perform Participant audits, including field audits, in accordance with the Information Systems Activity Review Policy (Policy # 20).
- 2.0 Investigation.** The ILHIE Authority, or its authorized designee, may conduct an investigation into potential noncompliance with these Policies and Procedures, the Data Sharing Agreement, or Applicable Law through audit or otherwise, resulting from a report, complaint or Participant self-disclosure, or by other means.
 - 2.1** A Participant shall cooperate in an ILHIE Authority investigation, including responding to information reasonable requests made by the ILHIE Authority.
- 3.0 Sanctions.** After an investigation, if the ILHIE Authority, or its authorized designee, determines that the evidence or other circumstances support the issuance of a notice of proposed action to a Participant, it may issue a notice that includes any or all of the following:
 - (i) The details regarding each instance of noncompliance with these Policies and Procedures, the Data Sharing Agreement or Applicable Law;
 - (ii) A proposed corrective action plan; or
 - (iii) Proposed sanctions, as set forth in the Sanction Policy (Policy #15).
- 3.1** After an investigation, if the ILHIE Authority, or its authorized designee, determines that a notice of proposed action is not appropriate given the lack of available evidence or other circumstances, it may issue one of the following:
 - (i) A letter finding that no action is recommended at that time; or
 - (ii) A letter finding that no action is warranted.

- 3.2** If a Participant who receives a notice of a proposed action from the ILHIE Authority agrees with the proposal, the Participant shall notify the ILHIE Authority of agreement in writing and shall promptly implement the action. The Participant shall provide the ILHIE Authority with implementation updates upon reasonable request. If the Participant fails to fully implement the action to the satisfaction of the ILHIE Authority, in its sole discretion, the ILHIE Authority may investigate the matter and issue a new notice of proposed action, and take other enforcement actions, as appropriate.
- 3.3** A Participant who receives a notice of proposed action from the ILHIE Authority may request an opportunity to show cause to the ILHIE Authority as to why the proposed action should not be implemented, in a manner consistent with the Data Sharing Agreement. The written request must be received by the ILHIE Authority within ten (10) business days of the Participant's receipt of the notice of proposed action. The ILHIE Authority may, in its sole discretion, determine whether it will reconsider the matter. If the matter is reconsidered, the ILHIE Authority may issue the same or a new notice of proposed action to the Participant, or may withdraw the notice of proposed action. A Participant may only request one opportunity to show cause under this Section.
- 3.4** A Participant's failure to comply with a notice of proposed action may result in enforcement actions by the ILHIE Authority.
- 4.0 Conflict.** If there is conflict between the terms of these Policies and Procedures and the terms of the Data Sharing Agreement, these Policies and Procedures shall control.
- 5.0 Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
- 5.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies & Procedures

42 U.S.C. §13410(e)
Data Sharing Agreement
Breach Notification and Mitigation
Compliant Handling and Resolution
Enforcement
Information Systems Activity Review
Sanctions

Definitions

Applicable Law
Breach

| |
|---|
| ILHIE Authority Participant Policies and Procedures |
|---|

| |
|--------------------------------------|
| Policies and Procedures |
| POLICY: Physical Safeguards |
| Policy #17 |
| Effective Date: April 2, 2014 |

Purpose: The ILHIE Authority is committed to preventing unauthorized physical access to workstations that can access Electronic Protected Health Information while ensuring that Authorized Users have appropriate access. Appropriate physical safeguards for the ILHIE Authority and Participants shall be those required by HIPAA, these Policies and Procedures, the Data Sharing Agreement and other Applicable Law.

Policy: The ILHIE Authority and Participants shall implement appropriate physical safeguards to prevent the inappropriate request, use, or disclosure of Electronic Protected Health Information other than as permitted by HIPAA, these Policies and Procedures, the Data Sharing Agreement and other Applicable Law. The ILHIE Authority encourages Participants to meet the HIPAA addressable specifications, to the extent deemed appropriate. All Authorized Users who use workstations will take all reasonable precautions to protect the confidentiality, integrity, and availability of Electronic Protected Health Information. This Policy and Procedure shall address the ILHIE Authority's physical safeguards and shall apply to the ILHIE Authority Workforce, contractors, Subcontractors and agents.

1.0 Facility Access Controls. The ILHIE Authority and Participants shall each implement policies and procedures to limit physical access to their respective electronic Information Systems, as defined in 45 C.F.R §164.304, and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

- 1.1** The ILHIE Authority and, to the extent required under HIPAA, Participants shall establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- 1.2** The ILHIE Authority and, to the extent required under HIPAA, Participants shall each implement policies and procedures to safeguard facilities and the equipment therein from unauthorized physical access, tampering and theft.
- 1.3** The ILHIE Authority and, to the extent required under HIPAA, Participants shall each implement procedures to control and validate a person's access to facilities based on that person's role or function, including visitor control, and control of access to software programs for testing and revisions.
- 1.4** The ILHIE Authority and, to the extent required under HIPAA, Participants shall each implement policies and procedures to document repairs and modifications to the physical components of facilities which are related to security (for example, hardware, walls, doors and locks).

- 2.0 Workstation Use.** The ILHIE Authority and Participants shall each implement policies and procedures, for each specific workstation or class of workstation that can access Electronic Protected Health Information, that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of the specific workstation or class of workstations.
- 3.0 Workstation Security.** The ILHIE Authority and Participants shall each implement physical safeguards for all workstations and other devices (including those accessed via secure, encrypted, remote access) that access Electronic Protected Health Information, to restrict access to Authorized Users.
- 3.1** Workstation security safeguards shall include password controls, including controls for physically unattended workstations, consistent with the User Authentication Policy (Policy #3).
- 4.0 Device and Media Control.** The ILHIE Authority and Participants shall each implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Electronic Protected Health Information into and out of a facility, and the movement of these items within the facility.
- 4.1** The ILHIE Authority and Participants shall each implement policies and procedures to address the final disposition of Electronic Protected Health Information, and/or the hardware or electronic media on which it is stored.
- 4.2** The ILHIE Authority and Participant shall each implement policies and procedures for removal of Electronic Protected Health Information from electronic media before the media are made available for re-use.
- 4.3** The ILHIE Authority and, to the extent required under HIPAA, Participants shall each maintain a record of the movement of hardware and electronic media and any person responsible therefore.
- 4.4** The ILHIE Authority and, to the extent required under HIPAA, Participants shall each create a retrievable, exact copy of Electronic Protected Health Information, when needed, before movement of equipment.
- 5.0 Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
- 5.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures:

The ILHIE Authority and, to the extent required under HIPAA, Participants will each comply with or implement the following procedures.

- 1.0** Information Systems and other electronic media containing Protected Health Information must be located and stored in secure environments that are protected by appropriate security barriers and entry controls.
- 2.0** Reasonable measures to prevent viewing Electronic Protected Health Information on workstations by unauthorized persons must be taken.
- 3.0** Regularly conduct a formal, documented process that ensures consistent control and protection of all electronic media and Information Systems containing Electronic Protected Health Information that is created, sent, received or destroyed.
- 4.0** Authorized Users who move electronic media or Information Systems containing Electronic Protected Health Information are responsible for the subsequent use of such items and must take all appropriate and reasonable actions to protect them against damage, theft and unauthorized access.
- 5.0** All Electronic Protected Health Information must be permanently removed from the hardware and electronic media on which the Electronic Protected Health Information is stored before the devices can be discarded or re-used.
- 6.0** Electronic Protected Health Information shall not be stored on removable media or portable workstation unless encrypted.

Associated Policies & References

45 C.F.R §164.310

Illinois Health Information Exchange System Security Plan (SSP)

User Authorization

Definitions

Authorized Users

Electronic Protected Health Information

HIPAA

ILHIE Authority

Information Systems

Participants

Subcontractors

Workforce

| |
|--------------------------------------|
| Policies and Procedures |
| POLICY: Encryption |
| Policy #18 |
| Effective Date: April 2, 2014 |

Purpose: This policy addresses HIPAA technical safeguard specifications regarding implementation of a mechanism to encrypt and decrypt Electronic Protected Health Information transmitted through or to the ILHIE. All data transmitted through the ILHIE or stored at rest in the ILHIE will be transmitted and stored in an encrypted form and will have controls to safeguard the integrity of the data.

Policy:

- 1.0 Encryption.** Any data transmitted through or stored in the ILHIE will be encrypted. The ILHIE Authority will use best efforts to assure that encryption and decryption technology is configured in accordance with industry and government best practices. The ILHIE Authority encourages Participants to meet the HIPAA Addressable encryption specifications for data maintained within the Participant's own Information Systems, to the extent deemed appropriate.
- 2.0 Compliance.** Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
 - 2.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures:

Participant Procedures

- 1.0** Each Participant will encrypt Electronic Protected Health Information provided to the ILHIE. Each Participant will decrypt Electronic Protected Health Information received from the ILHIE.
- 2.0** Each Participant will use best efforts to assure that it configures its encryption and decryption technology in accordance with industry and government best practices.

ILHIE Authority Procedures

- 1.0** The ILHIE Authority will implement encryption protocols according to current industry and government standards and implement updates consistent with industry and government best practices.
- 2.0** The ILHIE Authority will publish to its website the current encryption protocols in use by the ILHIE Authority.

Associated Policies & References

45 C.F.R §164.312(a)(2)(iv)

45 C.F.R §164.312(e)(1),(2)(ii)

45 C.F.R §164.530(c)

Compliance with Law and Policy

Illinois Health Information Exchange System Security Plan (SSP)

Definitions

Electronic Protected Health Information

ILHIE Authority

Information System

Participant



| |
|---|
| Policies and Procedures |
| POLICY: Risk Analysis and Management |
| Policy #19 |
| Effective Date: April 2, 2014 |

Purpose: This policy describes the risk analysis and risk management activities that the ILHIE Authority and Participants must perform in compliance with the HIPAA Security Rule requirements.

Policy: The ILHIE Authority and Participants shall each conduct security risk assessments to identify reasonably anticipated threats and vulnerabilities that present potential risk to the confidentiality, integrity and availability of Electronic Protected Health Information requested, used or disclosed through the ILHIE. The ILHIE Authority and Participants shall each develop security risk management plans to document the issues and concerns discovered in the risk assessment process, and document recommendations for addressing these concerns through the adoption and implementation of reasonable safeguards to protect Electronic Protected Health Information created, received, maintained or transmitted using the ILHIE technology and infrastructure.

1.0 Risk Analysis. The ILHIE Authority and Participants shall each conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of Electronic Protected Health Information held by the ILHIE Authority or the Participant, respectively, including risks related to the use of the ILHIE.

1.1 The identification, definition and prioritization of risks to ILHIE Authority technology and infrastructure will be based on a formal, documented risk analysis process.

1.2 The ILHIE Authority and Participants shall each re-assess risks, as needed, but no less than annually, after Security Incidents, Breaches, or both and as vulnerabilities are identified, respectively.

1.3 The ILHIE Authority shall re-assess its risks whenever significant changes occur in the ILHIE's information technology environment.

2.0 Risk Management. The ILHIE Authority and Participants shall each implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R §164.306(a) of the HIPAA Security Rule.

2.1 Selection and implementation of such security measures will be based on a formal, documented risk management process.

2.2 The ILHIE Authority and Participant will each evaluate and maintain security measures, periodically reviewing and updating the risk management plan in response to changes and risks identified through the risk analysis process.

3.0 Compliance. Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

3.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures, including providing documentation of the risk analysis results and risk management plan upon request.

Associated Policies & References

45 C.F.R 164.306(a)

45 C.F.R 164.308(a)(1)(ii)(A)

45 C.F.R 164.308(a)(1)(ii)(B)

Risk Management RFP

Definitions

Breach

Electronic Protected Health Information

ILHIE Authority

Participant

Security Incident

| |
|--|
| Policies and Procedures |
| POLICY: Information Systems Activity Review |
| Policy #20 |
| Effective Date: April 2, 2014 |

Purpose: Monitoring Information System events is an essential safeguard for the ILHIE infrastructure. ILHIE Authority audit logs permit the monitoring of Protected Health Information that is requested, used, or disclosure through the ILHIE and will be used for the purposes of monitoring the appropriateness of ILHIE access.

Only appropriately authenticated Authorized Users are granted access to the ILHIE. The ILHIE Authority can identify each Authorized User that has requested, used or disclosed an Individual's Protected Health Information through the ILHIE. Additional information about the request, use or disclosure of an Individual's Protected Health Information may be available from the Participant.

Policy:

1.0 Information Systems Activity Review. The ILHIE Authority and Participants shall each implement procedures to regularly review records of its respective Information System activity, such as audit logs, access reports, and Security Incident tracking and reporting, to identify potential inappropriate access and verify compliance with access controls.

1.1 The ILHIE Authority, or its authorized designee, shall perform regular audits of the acquisitions, access, uses or, disclosures of Protected Health Information through the ILHIE, and will conduct appropriate evaluations, including a risk assessment, when any major ILHIE Authority System or business changes are implemented.

1.2 The ILHIE Authority shall conduct penetration testing and compliance audits of the ILHIE Authority's Information System. The ILHIE Authority is authorized to conduct compliance audits of a Participant's System.

1.3 The ILHIE Authority and Participants will maintain an audit log for the period required by Applicable Law. The information will be housed in a retrievable storage medium.

1.4 Upon request, the ILHIE Authority will make its audit logs that pertain to a Participant available to such Participant.

2.0 Audit Protocol. The ILHIE Authority and Participants shall each generate audit logs in a standardized format such as ATNA to record respective System access and activity, and shall review the generated audit logs on a routine basis.

2.1 The ILHIE Authority shall implement Security Assertion Markup Language ("SAML") assertions as a component of the ILHIE audit log in accordance with the SAML Assertions and ILHIE Authority policy. Participant ability to

pass SAML-compliant user authorization information is a technical requirement for connecting to the ILHIE, effective June 30, 2014.

- 3.0 Detecting Security Incidents.** The ILHIE Authority and Participants shall each develop protocols to detect and identify System Security Incidents within their respective systems, in accordance with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.
- 3.1** The ILHIE Authority will address Security Incidents which utilize ILHIE technology or infrastructure or which allow unauthorized access to ILHIE technology, ILHIE infrastructure or Protected Health Information through the ILHIE in a timely manner.
- 3.2** Upon request and to the extent available, the ILHIE Authority will reasonably assist Participants in the procurement of additional detail not included in the ILHIE's standard audit log information, and assist the Participant in the investigation of any Security Incident suffered by the Participant, including the development and implementation of an appropriate corrective action plan.
- 4.0 Coordination.** The ILHIE Authority will coordinate any follow-up actions related to a Security Incident with the appropriate Participant(s) in accordance with the Data Sharing Agreement, these Policies and Procedures and Applicable Law.
- 5.0 Compliance.** Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with these Policies and Procedures.
- 5.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with and adherence to these Policies and Procedures.

Procedures

Participant Procedures

Participants will comply with or implement the following procedures.

- 1.0** Audit its Authorized Users' activities in order to assess potential risks and vulnerabilities with regard to Protected Health Information and use of the ILHIE.
- 2.0** Take appropriate corrective measures and document Security Incident findings in accordance with these Policies and Procedures, the Data Sharing Agreement and Applicable Law.

ILHIE Authority Procedures

The ILHIE Authority will comply with or implement the following procedures.

- 1.0** Audit its Authorized Users' activities in order to assess potential risks and vulnerabilities with regard to Protected Health Information and use of the ILHIE.

- 2.0** Take appropriate corrective measures and document Security Incident findings in accordance with these Policies and Procedures, the Data Sharing Agreement and Applicable Law.
- 3.0** Report a summary of the findings from ILHIE Authority System activity reviews to the ILHIE Authority Data Security and Privacy Committee as necessary, but at a minimum on an annual basis.

Associated Policies & Procedures

45 C.F.R § 164.308(a)(1)(ii)(D)

Accounting of Disclosures

Breach Notification and Mitigation

Data Sharing Agreement

Enforcement

SAML Assertions and ILHIE Policy

Sanctions

User Authentication

User Authorization

Definitions

Applicable Law

Audit Trail and Node Authentication

Audit Log

Authorized Users

Electronic Protected Health Information

Participant

Security Assertion Markup Language

Security Incident

System

| |
|--|
| Policies and Procedures |
| POLICY: Breach Notification and Mitigation Policy |
| Policy #21 |
| Effective Date: November 7, 2013 |

Purpose: HIPAA, HITECH, the Illinois Personal Information Protection Act (“PIPA”), and other Applicable Law require notice of a Breach. Should there be a Breach of Protected Health Information utilizing ILHIE technology or infrastructure, Breach notification and mitigation obligations may apply to both a Participant(s) and the ILHIE Authority, in its Business Associate capacity to Participants.

This Policy and Procedure establishes a Breach notification and mitigation protocol for Participants and the ILHIE Authority. It applies only to those privacy and security incidents which would qualify as a Breach under HIPAA, HITECH or other Applicable Law and which utilize ILHIE technology or infrastructure or which allow unauthorized access to ILHIE technology, ILHIE infrastructure or Protected Health Information through the ILHIE. The obligations contained herein comply with and supplement those obligations contained in HIPAA, HITECH or other Applicable Law. This policy shall be incorporated by reference into all existing and future Data Sharing Agreements entered into by and between Participants and the ILHIE Authority.

Policy: A Participant shall, promptly upon discovery of a Breach (whether a Breach of the ILHIE, or a Breach by the Participant, an Other Participant or the ILHIE Authority) report the Breach to the ILHIE Authority and the Affected Participants in accordance with this Policy and Procedure.

1.0 Participant Breach. A Breaching Participant shall, in accordance with its own policies, promptly investigate any and all Breaches. The Breaching Participant shall inform the ILHIE Authority and, in those cases where the Affected Participants can be identified, inform the Affected Participants of a Breach in accordance with the procedures set forth herein.

1.1 The Breaching Participant shall be responsible for notifying Individuals, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with those provided by any Affected Participant. An Affected Participant may also notify Individuals with whom the Affected Participant has or had a relationship and whose Protected Health Information was compromised by the Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that Affected Participants providing such notification shall use reasonable efforts to advise and coordinate any notice with the Breaching Participant, as well as the ILHIE Authority.

- 1.2** The Breaching Participant shall be responsible for mitigating the Breach. The ILHIE Authority shall have the right to participate in the investigation and to know the results and remedial action taken, if any, except that the ILHIE Authority need not be notified of specific workforce disciplinary actions and may not participate in any action or investigation by a Participant that would result in the loss of any applicable attorney-client privilege or work product protections. This Policy and Procedure shall not be interpreted in a way that would require a Participant to disclose Protected Health Information to the ILHIE Authority if such disclosure is not permitted under HIPAA, HITECH, or other Applicable Law.
- 2.0 ILHIE Breach.** The ILHIE Authority shall, in accordance with the procedures set forth herein, promptly upon discovery of any ILHIE Breach, report such ILHIE Breach to the Breaching Participant, as well as to the Affected Participants. The ILHIE Authority shall promptly investigate any ILHIE Breach, mitigate the ILHIE Breach, and cooperate with the Breaching Participant and all Affected Participants with respect to any mitigation, reporting or other obligations that the Breaching Participant, the Affected Participants or both may have. Each Breaching or Affected Participant shall be responsible for notifying Individuals to the extent required under HIPAA, HITECH, or other Applicable Law. The ILHIE Authority shall not give such notice unless and to the extent that a Participant has delegated to the ILHIE Authority the obligation to provide notice on behalf of that Participant. Notwithstanding the foregoing, the ILHIE Authority shall give any notice that it is required to provide under applicable law.
- 3.0 Role of ILHIE Authority.** Upon Breaching Participant request, the ILHIE Authority shall assist the Breaching Participant in identifying Affected Participants. Where multiple Participants are Breaching Participants or Affected Participants, upon the request of one or more Participants, the ILHIE Authority may coordinate communication and activities between those Participants, but nothing set forth in this Policy and Procedure shall require any Participant to delay its own investigation, reporting, or other activities that it deems necessary or appropriate to comply with Applicable Law or to assure the ongoing privacy and security of Protected Health Information. The ILHIE Authority shall not be responsible for making determinations as to which Participant is responsible for a Breach.
- 3.1** For all Breaches, an investigation of a Breach and all actions taken with respect to the Breach, shall be documented and provided to the ILHIE Authority by the Breaching Participant. The ILHIE Authority may use this information for education, policy, and the development of safeguards.
- 3.2** The ILHIE Authority shall prepare an annual report for Participants identifying Breaches which occurred within the previous year which utilized ILHIE technology or infrastructure, or which allowed unauthorized access to ILHIE technology, ILHIE infrastructure or Protected Health Information through the ILHIE. Nothing, however, precludes the ILHIE Authority from notifying Participants more frequently if the ILHIE Authority determines that doing so will be beneficial to ILHIE operations. The ILHIE Authority shall not disseminate or publish Protected Health Information. The ILHIE Authority may

disseminate or publish de-identified data to provide examples of Breaches for education, policy, and the development of safeguards.

- 4.0 Cooperation.** Participants shall appoint an individual to be contacted in the event of a Breach and shall notify the ILHIE Authority of this person and their contact information, including any changes thereto.
- 4.1** A Participant shall, promptly upon discovery of any Breach (whether a Breach of the ILHIE, or a Breach by the Participant, an Other Participant, or the ILHIE Authority) report by email the Breach to the ILHIE Authority and the Affected Participants. Participants are not responsible for monitoring the ILHIE or Other Participants for Breaches. Where a Participant reports an incident in good faith, the Participant will not be liable if the incident reported is subsequently determined not to be a Breach.
- 4.2** Participants shall cooperate in any good faith investigations conducted by the ILHIE Authority. Participants and the ILHIE Authority shall cooperate in any good faith investigations conducted by an Other Participant. In addition, a Participant shall cooperate with the legally required notification and mitigation activities of Other Participants or the ILHIE Authority.
- 5.0 Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
- 5.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.
- 6.0 Sanctions.** The ILHIE Authority may immediately suspend or revoke an Authorized User's ILHIE access for cause in accordance with the Sanction Policy (Policy #15) and the Data Sharing Agreement.

Participant Breach Procedures

- 1.0 Investigation.** A Breaching Participant shall, in accordance with its own policies, promptly investigate suspected or actual reported Breaches.
- 2.0 Notifying the ILHIE Authority and Affected Participants ("Informational Notification").** A Breaching Participant shall notify the ILHIE PCO and, in those cases where the Affected Participants can be identified, the Affected Participants of a Breach. The ILHIE Authority shall make Participant contact information available to all Participants to facilitate informational notification. No notification is required regarding the ongoing existence, occurrence or attempt of unsuccessful security incidents, including pings and other broadcast attacks on a Participant's firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized acquisition, access, use, or disclosure of Protected Health Information.

- 2.1** Informational Notification shall be made promptly, but in no event more than five (5) business days from discovery of a Breach. Notification shall be made irrespective of whether the Breaching Participant's investigation is complete.
- 2.2** Informational Notification shall be done (i) via email or (ii) via phone conference with the ILHIE PCO and Affected Participants, provided that notice by email is subsequently provided to all Affected Participants and the ILHIE PCO.
- 2.3** Informational Notification shall include sufficient information so that the ILHIE PCO, if requested by a Participant, can assist the Participant in its investigation and mitigation efforts. Informational Notification should include, but need not be limited to, the items set forth on Exhibit 1 to the extent that the Breaching Participant has knowledge of such items.
- 2.4** Upon determination that a previously reported Breach is not a Breach, the Participant that reported the Breach shall send an updated status to the ILHIE Authority and Affected Participants.
- 3.0** *Notification Required by Law ("Legal Notification").* Except as provided in the ILHIE Authority Breach Procedures Section, the Breaching Participant shall, at its expense, be responsible for notifying Individuals, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with the Affected Participant(s). An Affected Participant may also notify Individuals with whom the Affected Participant has or has had a relationship and whose Protected Health Information was compromised by the Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that Affected Participants providing such notice shall use reasonable efforts to advise and coordinate any notice with the Breaching Participant and the ILHIE Authority.
- 4.0** *Mitigation and Remediation.* The Breaching Participant shall take reasonable steps to pursue, address, and mitigate any Breach which has resulted from its acts or omissions, which may include a request to any party who improperly received such information to return and/or destroy the impermissibly disclosed information.

 - 4.1** The Breaching Participant shall assume mitigation costs incurred by itself and the ILHIE Authority and Affected Participants, which were caused by the Breach of the Breaching Participant. Mitigation costs shall not include special, consequential, indirect, exemplary, or punitive damages as further described in the Data Sharing Agreement. The Breaching Participant(s), the ILHIE Authority, and any Affected Participant(s), shall coordinate mitigation efforts to minimize duplication of efforts. Disputes with respect to this Section shall be resolved in accordance with any dispute resolutions mechanism set forth in the Data Sharing Agreement.

- 5.0** *Reporting Requirements.* The investigation of a Breach and all actions taken with respect to the Breach shall be documented, and the documentation shall be provided by the Breaching Participant to the ILHIE Authority within thirty (30) days of the provision of Legal Notification to Individuals. The documentation should include, but need not be limited to, the items set forth on Exhibit 2, to the extent that the Breaching Participant has knowledge of such items. The ILHIE Authority need not be notified of specific workforce disciplinary actions and may not participate in any action or investigation by a Participant that would result in the loss of any applicable attorney-client privilege or work product protections. This Policy and Procedure shall not be interpreted to require any Participant to disclose any Protected Health Information to the ILHIE Authority if such a disclosure would not be permitted under HIPAA, HITECH, or other Applicable Law.
- 6.0** *Role of ILHIE Authority.* If multiple Participants cannot agree on which is the Breaching Participant, on the request of one or more Participants, then the ILHIE Authority may facilitate the resolution of the matter.
- 6.1** The ILHIE Authority shall facilitate conference calls and other mechanisms to help Participants coordinate their responses and communications regarding Breaches to ensure that all such Participants are aware of mitigation efforts and costs, and to ensure that the Breach is generally described in the same way in press releases and government filings.
- 6.2** The ILHIE Authority shall develop template documents to facilitate communication of Breaches to Individuals, the Department of Health and Human Services, and the media, as well as other Individuals or entities requiring notification pursuant to HIPAA, HITECH, or other Applicable Law. Use of such templates is not required.
- 6.3** The ILHIE Authority may suspend or revoke an Authorized User in accordance with the Sanction Policy (Policy #15) and the relevant Participant's Data Sharing Agreement.
- 6.4** All Protected Health Information that the ILHIE Authority receives, or to which it has access in connection with any Breach, shall be subject to the requirements of its Business Associate Agreement(s) with Participant(s) and to HIPAA, HITECH, or other Applicable Law.
- 6.5** The ILHIE Authority shall take all action necessary to prevent any Protected Health Information that it receives in connection with a Breach from being subject to disclosure or release under the Illinois Freedom of Information Act (5 ILCS 140/1 *et seq.*) or similar federal or Illinois law or regulation requiring disclosure of government records or information.

ILHIE Breach Procedures

- 1.0** *Investigation.* The ILHIE Authority shall, in accordance with its own policies, promptly investigate actual or suspected ILHIE Breaches.

- 2.0** *Informational Notification.* The ILHIE Authority shall inform the Breaching Participant, as well as Affected Participants, of an ILHIE Breach. No notification is required regarding the ongoing existence and occurrence or attempts of unsuccessful security incidents, including pings and other broadcast attacks on the ILHIE's firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized acquisition, access, use, or disclosure of Protected Health Information.
- 2.1** Informational Notification shall be made as soon as possible, but in no event more than five (5) business days from discovery of the ILHIE Breach. Notification shall be made irrespective of whether the ILHIE Authority's investigation is complete.
- 2.2** Informational Notification shall be made (i) via email or (ii) via phone conference with the ILHIE PCO, Breaching Participant, and Affected Participants, provided that an email notice is subsequently provided to all parties.
- 2.2** Informational Notification shall include sufficient information so that each Participant that receives notification can conduct its own investigation and mitigation efforts. Informational Notification should include, but need not be limited to, the items set forth on Exhibit 1, to the extent that the ILHIE Authority has knowledge of such items.
- 2.3** Upon a determination that a previously reported ILHIE Breach is not Breach, the ILHIE Authority shall send an updated status to any Breaching Participants and Affected Participants.
- 3.0** *Notification Required by Law ("Legal Notification").* A Breaching Participant shall be responsible for notifying Individuals, the Department of Health and Human Services, and, if necessary, the media, as well as other entities, if such notice required under HIPAA, HITECH, or other Applicable Law, about an ILHIE Breach; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with any Affected Participant. An Affected Participant may also notify Individuals with whom the Affected Participant has or had a relationship and whose Protected Health Information was compromised by the ILHIE Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that Affected Participants providing such notification shall use reasonable efforts to coordinate any notice with and advise any Breaching Participant and the ILHIE Authority. The Breaching and Affected Participants may delegate to the ILHIE Authority notification of Individuals about an ILHIE Breach on the Breaching Participant's or Affected Participant's behalf. The ILHIE Authority shall pay for the costs of Individual notification pertaining to an ILHIE Breach incurred by either the Breaching Participant, the Affected Participant, or by the ILHIE Authority on behalf of the Breaching Participant or Affected Participant.
- 4.0** *Mitigation and Remediation.* ILHIE Authority shall take reasonable steps to pursue, address, and mitigate any ILHIE Breach, which may include a request to the party

who improperly received such information to return or destroy the impermissibly disclosed information.

- 4.1** In accordance with the terms of the Data Sharing Agreement and Applicable Law, the ILHIE Authority shall assume mitigation costs incurred by itself, Breaching Participants and Affected Participants and which were caused by an ILHIE Breach. Mitigation costs shall not include special, consequential, indirect, exemplary, or punitive damages as further described in the Data Sharing Agreement. The ILHIE Authority, Breaching Participants and any Affected Participants shall coordinate mitigation efforts to minimize duplication of efforts. Disputes with respect to this Section shall be resolved in accordance with the dispute resolution mechanism set forth in the applicable Data Sharing Agreement.
- 5.0** *Reporting.* An investigation of an ILHIE Breach and all actions taken with respect to the ILHIE Breach by the ILHIE Authority shall be documented, and the ILHIE Authority shall provide such documentation to any Breaching Participant and Affected Participants within thirty (30) days of the provision of Legal Notification to Individuals. Documentation should include, but need not be limited to, the items set forth in Exhibit 2, to the extent that the ILHIE Authority has knowledge of such items.
- 6.0** *Coordination between Participants.* ILHIE Authority shall perform the role set forth in the Participant Breach Procedures Section of this Policy with respect to ILHIE Breaches.

Associated Policies and References

Data Sharing Agreement
45 C.F.R §164.400 et seq.
Public Law 111-005
Personal Information Protection Act, 815 ILCS 530/

Exhibits

| |
|--|
| EXHIBIT 1: INFORMATIONAL NOTIFICATION REQUIREMENTS |
|--|

To the extent known, the following information shall be submitted to the ILHIE Authority as well as other Affected Participants upon the discovery of a Breach or suspected Breach.

1. Date of Breach or suspected Breach.
2. Date of discovery.
3. Description of Breach or suspected Breach. Please be specific and include the number of Individuals affected.
4. Description of Protected Health Information acquired, accessed, used, or disclosed. Please be specific as to the type of information.
5. Whether or not the following Protected Health Information was included in the unauthorized acquisition, access, use, or disclosure as well as explanatory details:
 - ☐ HIV/AIDS information including whether an HIV test was administered
 - ☐ genetic testing or counseling information
 - ☐ alcohol or substance abuse information
 - ☐ mental health and developmental disability information
6. Whether or not the following information was included (in whole or in part) in the unauthorized acquisition, access, use, or disclosure as well as explanatory details:
 - ☐ Social security number
 - ☐ Driver's license or State ID number
 - ☐ Account number, or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account
7. Recipient of unauthorized acquisition, access, use, or disclosure (include full identification, address, email, and phone number).
8. Description of any actions taken thus far with respect to investigation and mitigation efforts.

| |
|---------------------------------------|
| EXHIBIT 2: BREACH REPORT REQUIREMENTS |
|---------------------------------------|

To the extent known, the following information shall be submitted to the ILHIE Authority as well as other Affected Participants within thirty (30) days of the provision of Legal Notification to Individuals.

1. Date of Breach.
2. Date of discovery.
3. Description of Breach. Please be specific and include the number of Individuals affected.
4. Description of Protected Health Information acquired, accessed, used, or disclosed. Please be specific as to the type of information.
5. Whether or not the following Protected Health Information was included in the unauthorized acquisition, access, use, or disclosure as well as explanatory details:
 - ☐ HIV/AIDS information including whether an HIV test was administered
 - ☐ genetic testing or counseling information
 - ☐ alcohol or substance abuse information
 - ☐ mental health and developmental disability information
6. Whether or not the following information was included (in full or in part) in the unauthorized use or disclosure as well as explanatory details:
 - ☐ Social security number
 - ☐ Driver's license or State ID number
 - ☐ Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account
7. Recipient of unauthorized acquisition, access, use, or disclosure (include full identification, address, email, and phone number).
8. Description of investigation.
9. Description of all applicable mitigation actions, including, but not limited to:
 - ☐ Retrieval of Protected Health Information
 - ☐ Whether or not disciplinary action was taken. NOTE: Specific details are not required

- ❑ Technical modifications
- ❑ Administrative modifications (e.g., adoption or modification of policies, workflow processes, etc.)
- ❑ Physician modifications
- ❑ Retraining
- ❑ Credit monitoring provided to Individuals
- ❑ Other

10. Date notification provided to Individuals.

11. Date notification provided to the Department of Health and Human Services.

12. Date notification provided in media (if required).

Definitions

Affected Participant
 Authorized User
 Breach(es)
 Breaching Participant
 Department of Health and Human Services
 HIE
 HIPAA
 HITECH
 ILHIE
 ILHIE Authority
 ILHIE Breach
 ILHIE PCO
 Informational Notification
 Legal Notification
 Participant
 System

| |
|--------------------------------------|
| Policies and Procedures |
| POLICY: Contingency Plan |
| Policy #22 |
| Effective Date: April 2, 2014 |

Purpose: The ILHIE Authority is committed to ensuring the confidentiality, integrity and availability of Electronic Protected Health Information created, received, maintained or transmitted through the ILHIE, including in preparing for and responding to emergencies or disasters.

Policy:

- 1.0 Contingency Plan.** The ILHIE Authority and Participants shall each establish (and implement, as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, System failure and natural disaster) that damages an Information System containing Electronic Protected Health Information and which is part of or connected to the ILHIE.
- 2.0 Compliance.** Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.
 - 2.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures

Participant Procedures

- 1.0** In accordance with HIPAA, each Participant shall implement a contingency plan that includes the following:
 - (i) Data backup plan procedures to create and maintain retrievable exact copies of Electronic Protected Health Information;
 - (ii) Disaster recovery plan procedures to restore any loss of data (as needed); and
 - (iii) Emergency mode operation plan procedures to enable continuation of critical business processes for protection of the security of Electronic Protected Health Information while operating in emergency mode.

Each Participant shall implement the following Addressable implementation specifications to the extent deemed necessary by the Participant in accordance with HIPAA:

- (i) Testing and revision of procedures for periodic testing and revision of contingency plans; and

- (ii) Applications and data criticality analysis to assess the relative criticality of specific applications and data in support of other contingency plan components.

ILHIE Authority Procedures

1.0 In accordance with HIPAA, the ILHIE Authority, or its authorized designee, shall implement a contingency plan that includes the following procedures and analyses:

- (i) Data backup plan procedures to create and maintain retrievable exact copies of Electronic Protected Health Information;
- (ii) Disaster recovery plan procedures to restore any loss of data (as needed);
- (iii) Emergency mode operation plan procedures to enable continuation of critical business processes for protection of the security of Electronic Protected Health Information while operating in emergency;
- (iv) Testing and revision of procedures for periodic testing and revision of contingency plans; and
- (v) Applications and data criticality analysis to assess the relative criticality of specific applications and data in support of other contingency plan components.

Associated Policies & Procedures

45 C.F.R §164.308(a)(7)(i)-(ii)

Illinois Health Information Exchange System Security Plan (SSP)

Definitions

Electronic Protected Health Information

HIPAA

ILHIE Authority

Participant